AN EVALUATION OF THE EFFECTIVENESS OF ACCESS CONTROL MEASURES WITHIN THE MANGAUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICES

by

LETSHEGO ANDREW MANELE

Submitted in accordance with the requirements for the degree of

MAGISTER ARTIUM

in the subject

SECURITY MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF K PILLAY

November 2021

COPYRIGHT

UNISA

2021

DECLARATION

Name: **LETSHEGO ANDREW MANELE**

Student number: **36872121**

Degree: **Magister Artium in Criminal Justice (Security Management)**

AN EVALUATION OF THE EFFECTIVENESS OF ACCESS CONTROL MEASURES WITHIN THE MANGAUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICES

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

15 November 2021

SIGNATURE DATE

DEDICATION

In memory of my grandfather, Mr Ntulo George Manele, my grandmother, Mrs Elizabeth Nontsokolo Manele, my Father, Mr Tshepiso April Manele and my Mother Mrs Alina Ntombizodwa Manele who perceived that one-day deliverables will be realised.

ACKNOWLEDGEMENTS

I would like to thank God, the almighty for his wisdom, strength, perseverance and guidance throughout my journey in the completion of this dissertation.

I would like to acknowledge the following individuals who contributed in helping me complete this study.

- To my family members, my lovely wife Dihedile for her enormous support and understanding, my daughters Ntombizodwa and Nthabiseng and my son Letshego.
- My supervisor, Prof Krisandren Pillay. I wish to thank him for his mentorship, guidance and support and for believing in me. Most of all I thank you for assistance, as an expert in the field of Security Management.
- My colleagues in the Mangaung Metropolitan municipality, Mr N Maswabi, my supervisor, I thank you for time offs to attend workshops for M&D, Messrs B Swart and GP Venter for their expert advises in security matters and finally, A Jenkinson, the Manager: E-Governance who assisted me with the formatting and layout of this dissertation.

EXECUTIVE SUMMARY

This study evaluated the effectiveness of access control within the Mangaung Metropolitan municipality regional offices in Bloemfontein, Botshabelo and Thaba Nchu. The aims and objectives of the research study are to examine the effectiveness of the existing access control measures currently in place within the three regional offices of the Mangaung Metropolitan Municipality to; evaluate the security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality regional offices at access control points. Lastly, to make recommendations on the types of access control measures used to mitigate the impact of the risk factors.

The researcher used the qualitative approach where one on one interviews were conducted with forty- five (45) participants using the interview schedule. The researcher used the purposive sampling technique in which participants were selected on the basis of their knowledge of access control measures in their regional offices as well as a snow-ball sampling in which other employees recommended to the researcher participants to be included in the study.

The study revealed that access control measures that are currently in place in the three regional offices are inadequate and ineffective; the three regional offices are vulnerable due to their probable exposure to security risks such as theft, armed robbery and cash in transit heist. Lastly, an integrated access control measures comprising physical, electronic, administrative and biometric technology are proposed to authenticate the identity of people entering the premises of the regional offices.

The study proposes future research on client satisfaction with aspect of access control to solicit their perception, feeling and experience of members of the community of the effectiveness of access control in regional offices during their daily visits; Future study to be conducted in all buildings and premises of the Mangaung Metropolitan municipality to implement a standard and uniform system for access control. Lastly, a research to be conducted to assess the effectiveness of physical security in totality at all government offices not only one aspect such as access control.

Dipatlisiso tse di sekaseka bokgoni ba megwa ya go laola matseno mo dikagong tsa dikantorong tsa sedika tsa Bloemfontein, Botshabelo le Thaba Nchu tsa masepala wa Mangaung. Maikaelelo a dipatlisiso tse ke go seseka bokgoni ba thulanyo ya matseno mo dikagong tsa dikantoro tsa sedika tsa masepala wa Mangaung, go bontsha dikotsi tse , baberiki le sechaba di lebaganeng le tsona mo mafelong a go tsena mo dikantorong tsa sedika, sa bofelo go dira tshwaelo ka ditsela tse di maleba go laola matseno mo dikantorong tsa sedika tsa Mangaung.

Mobatlisisi o tlhopile batsaya karolo ba shome nne le botlhano (45) go ralala le dikantoro tsa sedika tsa masepala wa Mangaung. Batsaya karolo ba tlhopilwe mabapi le kitso ya bona ya taolo ya matseno mo meagong le dikantorong le go latela tlhagisiwa ke batho ba bangwe. gore ba tsenyiwe mo dipatlisisong.

Dipatlisiso tse di tlhagisitse gore dikantoro tsa sedika tsa masepala wa Mangaung di mo kotsing thata ka ntlha ya ditlolo molao tse di tshwana le go utswa, go dirisa digoka go tsaya dilo tsa masepala le go tlhasela dikoloi tse di tsamaisang madi a patalwang ke maloko a sechaba go bona diterelo mo masepaleng. La bofelo dipatlisiso di tlhagisitse gore taolo ya matseno mo dikantorong tse tsa sedika tsa mangaung e ka tokafala fa e ka dirisa lenane le le tlhakaneng jaaka ditsela tsa seteginiki.

Mo isagong ya go laola go tsena ga batho mo dikagong tsa masepala tsa Mangaung, dipatliso di eletsa gore go tsenyiwe maloko a sechaba se se berekisang dikago tsa masepala gore ba hane ka dikeletso mabapi le taolo ya matseno mo dikagong , dipatlisiso di tsenye meago yotlhe ya masepala le dikago tsotlhe tsa puso ka kakaretso.

Dipatlisiso tsena di lekola bokgoni ba tsela ya ho laola makeno meahong ya dikantoro tsa sedika tsa Bloemfontein,Botshabelo le Thaba Nchu tse ka hara masepala wa Mangaung. Maikemisetso a dipatlisiso ke ho lekola bokgoni ba mehato ya makeno meahong ya dikantoro tsa sedika sa masepala wa Mangaung, Ho lekola dikotsi tse basebetsi le sechaba di tobaneng le tsona dibakeng tsa ho kena dikantorong, sa ho qetela ho etsa tshwaelo ya ditsela tse tsepameng mabapi le ho laola makeno dikantorong tsa sedika sa masepala wa Mangaung.

Mobatlisisi o kgethile ba nka karolo ba le leshome nne le bohlano (45) ho ralalla le dikantoro tsa sedika tsa masepala wa Mangaung. Ba nka karolo ba ile ba khethiwa ho latela tsebo ya bona ya taolo ya makeno meahong le dikantorong le ho thongwa ke batho ba bang hore ba kenywe dipatlisisong.

Dipatlisiso di hlahitse hore dikantorong tsa sedika sa masepala wa Mangaung di kotsing kapo di hlokolotsing tlolong ya molao tse tshwanang le ho utswa, ho sebedisa digoka ho nka thepa ya masepala le ho hlasela dikoloi tse tsamaisang chelete.La ho qetela dipatlisiso di hlahisistse hore taolo ya makeno dikantorong tsa sedika tsa Mangaung e tshwanetse ho kenya lenane le kopaneng jwala ka la seteginiki.

Nakong e tlang ya ho laola ho kena ha batho meahong ya masepala, dipatlisiso di lakatsa hore ho keniwe sechaba se sebedisang meaho ya masepala ho fumane keletso ya ho laola makeno meahong , dipaltiliso di akaretse meaho kaofela le dikaho tsohle tsa puso.

Key words: Access control, metropolitan municipality, security measures, security risk, protection, vulnerability, crime, theft, biometric.

ABBREVIATIONS

ANPR	Automatic Number Plate Recognition
ASIS	American Security Industries Association
BSIA	British Security Industries Association
CCTV	Close circuit television
CIA	Confidentiality, Integrity and Availability
CISSP	Certified Information System Security Professionals
DAC	Discretionary Access Control
FBI	Federal Bureau of Investigation
HSPD	Homeland Security Presidential Directive
ID	Identity Document
IDP	Integrated Development Plan
MAC	Mandatory access control
MMC	Member of the Mayoral Committee
MMM	Mangaung Metropolitan Municipality
NIST	National Institute of Standards and Technology
NQF	National Qualifications Framework
PAC	Personal Access Code
PIN	Personal Identification Number
RBAC	Role –Based Access Control
RFID	Radio Frequency Identification
SALGA	South African Local Government Association

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1
INTRODUCTION AND MOTIVATION FOR THE RESEARCH

1.1 INTRODUCTION

The Mangaung Metropolitan Municipality, which is located in the Free State Province was established in 2011 in terms of the Municipal Structures Act. No 117 of 1998. According to this Act, it is classified as a category (A) municipality which exercises both the executive and legislative powers (Municipal Structures Act 117 of 1998, section 12). It operates within its powers and functions as determined by the Constitution of the Republic of South Africa 1996, (Act 108 of 1996), (Section 152).

The Mangaung metropolitan area is made up of the following six former municipal areas in Free State Province: Bloemfontein; Botshabelo; Thaba Nchu; Wepener; Dewetsdorp and Van Stadensrus covering 6863 square kilometres and has a population of 826979 residents (Stats SA 2016:11). These former municipalities consisted of the Mangaung local municipality and Motheo District municipality. After the 2016 local government election, Naledi local municipality and the town of Soutpan were incorporated (Mangaung Metropolitan Municipality. The Integrated Development Plan, 2018/19: 40).

Mangaung Metropolitan Municipality depends on its human capital, information and assets to deliver services and ensure the safety and security of its stakeholders. It must therefore manage these resources with due diligence and take appropriate measures to protect them (Mangaung Metropolitan Municipality. Integrated Development Plan, 2018/19: 40).

One of the most significant security measures used to ensure the optimal realisation of the above is access control (Artkinson,2018: n.p.). At Mangaung Metropolitan Municipality offices, access control is used as a security measure to restrict access of unauthorised people to the buildings and premises. These security measures are implemented to protect organisations from risks relating to the loss of assets, personal injury and damage to property and to lower the impact of losses and damage to the organisation (Hessel 2018: 2).

The study was undertaken due to a rising number of security breaches occurring at the Mangaung metropolitan municipal offices despite the prevalence of various access control system. These include amongst others: unlawful movement and removal of cash, valuables and sensitive documents within and out of the head office, regional offices and other organisations.

1.2 PROBLEM STATEMENT

The Mangaung Metropolitan Municipality owns assets with a total value of R1.4 billion (Mangaung Metropolitan Municipality Assets Register, 2019). These cover fixed assets such as buildings and movable assets, for example, the municipal vehicle fleet, heavy plant machinery and equipment. Others include immovable assets such as the water and sanitation network, land, roads, landfill sites and quarries, intangible assets such as servitude, computer software and hardware; heritage sites, conservation areas and zoo animals (Mangaung Metropolitan Municipality assets register, 2019).

Between 2011 and 2016, the Mangaung Metropolitan Municipality suffered numerous financial and physical losses as a result of security breaches (Mangaung Metropolitan Municipality Risk register, 2017/18). This caused serious financial and reputational losses estimated at R350 million over the last five years, caused by inadequate and ineffective physical access control measures within these offices (Mangaung Metropolitan Municipality Asset Register 2016). Common security breaches were unauthorised access to buildings and premises, theft, armed robbery, vandalism, damage to property and threats to the safety of both employees and visitors (Mangaung Metropolitan Municipality Risk Register, 2017/18).

The following examples illustrate the extent of financial losses suffered by the metropolitan municipality from 2015 until 2018.

In 2015 a newly purchased metropolitan municipality vehicle fleet to the value of R100m was stolen at the mechanical workshop together with the disappearance of a number of vehicles that were sent for repairs. In addition, a number of burglaries at the IT offices and the head office led to the theft of computer amounting to millions of rands and laptops stolen from the offices (Mangaung Metropolitan Municipality Risk register 2015).

On 4 July 2018, a group of criminals entered the Bloemfontein regional office undetected and attempted to take an undisclosed amount of revenue and held the personnel hostage (Gericke, 2018:1).

On 26 July 2018, a group of disgruntled employees gained unlawful access to the payroll offices undetected and attacked the staff over the overtime and stand-by allowances that had not been added to their salaries at the end of that month (Mangaung Metropolitan Municipality Law enforcement crime report, 2018: n.p.). Given the extent of the losses sustained by the Mangaung Metropolitan Municipality, these examples show that employees, clients, contractors and stakeholders do not feel safe when they enter the municipality offices (Bowers, 1988:14), thereby prompting further evaluation of the problem.

1.3 RATIONALE FOR THE STUDY

The study was motivated by the researcher's observation that the Mangaung Metropolitan Municipality's regional offices experienced several security breaches due to a lack of the implementation of effective access control measures.

The rising number of security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality regional offices as a result of security breaches, prompted a deeper investigation into the problem.

A further reason to conduct the study was the researcher's interest to reduce and minimise losses sustained as a result of ineffective access control measures. These can have both financial and reputational impacts on the Mangaung Metropolitan Municipality and its regional offices in meeting their service delivery mandate. Furthermore, the researcher who is currently employed at Mangaung Metropolitan Municipality gained many years of experience in the provision and management of contract security services to both the government and the private sector specialising in both guarding and access control. This experience and observation by the researcher added further impetus for the study.

1.4 AIM AND OBJECTIVES OF THE STUDY

1.4.1 Aim of the study

Any research process aims to establish facts through the accumulation of data in order to determine the authenticity of a given situation under study (Mouton, 1996:103). This study seeks to evaluate the effectiveness of access control systems at the Mangaung Metropolitan Municipality's regional offices.

1.4.2 Objectives of the study

The study will focus on the following objectives based on the on-going security threats and risks occurring at access control points at the Mangaung Metropolitan Municipality's regional offices.

The objectives of the study are to:

- examine the effectiveness of the existing access control measures currently in place within the three regional offices of the Mangaung Metropolitan Municipality.
- evaluate the security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality's regional offices at access control points.
- make recommendations on the types of access control measures used to mitigate the impact of risk factors.

1.5 RESEARCH QUESTIONS

Based on these objectives, the study will seek to address the following research questions:

- what are the existing access control measures currently in place at the Mangaung Metropolitan Municipality's regional offices?
- what are the security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality 's regional offices as a result of ineffective access control or a lack of access control measures?

- which types of access control measures can be implemented to eliminate security breaches within Mangaung Metropolitan Municipality regional offices?

1.6 VALUE OF THE RESEARCH

Due to persistent security breaches attributed to unauthorised ingress and egress by both the public and the private sector at the Mangaung Metropolitan municipal offices, a long-term benefit of the study is to broaden the theoretical and technical knowledge required by Mangaung Metropolitan Municipality management, to implement effective access control measures that will mitigate the effects of security breaches attributed to unauthorised entry into the facility.

The research will provide management of the Mangaung Metropolitan Municipality and its regional offices with empirical data to support expenditure in security measures by providing additional knowledge for the implementation of coordinated access control, that will continuously monitor, prevent and detect security breaches confronting their organisations.

It will assist in the building of capacity at the Mangaung Metropolitan Municipality and in this way, help to reduce the incidence of security risks through an integrated access control system to enhance their success in service delivery mandates by reducing their operating costs through reduced losses.

The study will promote community confidence in the Mangaung Metropolitan Municipality which through the implementation of effective access control measures, will guarantee them regular provision of services, and also ensure their safety during their daily visits to the regional offices for their service delivery needs and the payment of their rates and taxes. It will add value to both employees and clients of the regional offices who will benefit from a safe and secure environment and by empowering management through legislation and recent technology to be more effective in the fight against crime.

It will contribute a point of reference in academic conversation in the field of Security Science and it will serve as a platform for future research of effective access control.

Finally, it will demonstrate the benefits of the application of access control to other municipalities as a measure to curb the losses and to promote the safety of the employees, stakeholders and clients.

1.7 LIMITATIONS OF THE STUDY

The researcher identified several limitations whilst undertaking the current study.

During the data collection phase, the proclamation of the Disaster Management Act 2002 (Act No 57 of 2002) by the President of South Africa, Cyril Ramaphosa on 26 March 2020, placed the country under lockdown level five. As a result, various employment sites and employees except for essential services were allowed to come to work and other employees and their various workplaces were closed. The Mangaung Metropolitan municipality regional offices were placed under lock down until October 2020 and this had an impact on the data collection process for the study because the participants, who are employees in those regional office were at home.

The respondents whom the researcher had purposively selected for participation in the study due to their vast experience with the application of access control in their respective regional offices worked from home, as a result of comorbidities and others due to age. This had a great influence on the data collection since some of the participants did not want close contact with the researcher for fear of contracting the virus. Though he was able to visit some at their respective homes, others simply did not want that contact due to their fear of contracting the virus. To mitigate this, the researcher assured them that he will adhere to the Covid 19 government protocols before visiting them.

Another drawback is that the findings cannot be a true reflection of an entire population since a limited sample comprising forty- five participants from a population of five thousand (5000) employees working at the Mangaung Metropolitan municipality participated in the study. In addition, the interview process was often disrupted by members of the community seeking assistance from officials during the interview.

The communities regard the regional offices as the face of service delivery. Some participants were not keen to be recorded as they were worried that they might divulge certain information which might compromise them with their superiors. The researcher assured them that permission for their taking part was authorised by the City Manager and UNISA.

1.8 DEFINITION OF KEY TERMS

1.8.1 Metropolitan municipality

A Metropolitan municipality is a category of a municipality consisting of a number of towns established to coordinate the delivery of service to the whole area. These services include governance of the affairs of its citizens through promulgation and administration of by-laws, provision of basic services to the community, promotion of local economic development and fostering community participation in the planning and budgetary process (The Constitution of RSA 1996, Act 108, section 152).

1.8.2 Access control

Access control is a process of regulating and restricting the movement of people into buildings and premises and the verification of their identities, to determine whether they are allowed entry in or denied exiting from the building (Malik (2016: 2). According to Kole (2014:7), access control can be implemented through gates, doors, ID cards, badges, visitor escorts, turnstiles, keypads, card readers, the biometric system, X-ray machines, metal detectors, vehicle traps, security personnel and procedures. It can be a stand-alone or integrated with CCTV and an intrusion alarm system. At the Mangaung Metropolitan Municipality, current access control measures are security personnel, turnstiles, biometric system, gates, fence, CCTV, keypads and doors.

1.8.3 Mandatory access control (MAC)

Mandatory access control is a measure using security clearance issued to employees by the organisation to enter a certain area within a facility (Conrad, 2012:9). Harris (2013: 9) holds the view that employees' access to different areas in a facility depends on the level of clearances given, that draws a need to know principle, which entails restricting knowledge and information of something only to certain people as a security precaution. At the Mangaung Metropolitan Municipality, this applies to access to organizational servers which are restricted only to certain officials such as the Chief Information Officer and Chief Technology Officer.

1.8.4 Discretionary access control (DAC)

Discretionary access control is the level of access to a facility given to individuals with discretion by the owner of the facility according to their various responsibilities (Harris, 2013:9). Only permitted persons and authorised users of the system are given access to the object and it prevents access to those not given permission and authority. An example of this, is access into fire arm safes of the Mangaung Metropolitan Municipality, which is restricted only to the Designated Fire Arm Officer (DFO).

1.8.5 Role-based access control (RBAC)

Role-based access control is the level of access given to an individual based on and restricted to the role of the individual within the organization. Access to facilities depends on the assignment given to active and authorised users of the system, which is based on the member's affiliation to an organisation (Harris, 2013: 19). An example is access given to certain individuals at the water reservoirs, reticulation and treatment centres of the Mangaung Metropolitan Municipality.

1.8.6 Security measures

Security measures are defined as the implementation of protection measures such as human, technological, policy and procedure and physical security aids to prevent losses and protect the premises against security threats (Nkwana, 2015 :8).

1.8.7 Security Risk

Security risk is defined as potential loss resulting from lax security and protection measures that indirectly and directly cause damage and financial losses to an organization (Kole, 2015: 12). Examples of these security risks confronting the organisations include burglary, theft, armed robbery, sabotage and damage to property. Purpura (2013: 264) provides a different meaning of risk by defining the latter as the measure of the frequency, probability and impact from exposure to threats and hazards.

1.8.8 Vulnerability

This is the level of exposure to security risks and hazards to which the organisation may be subjected to as a result of inadequate and ineffective security measures (Norman, 2015 :156). Examples of physical vulnerabilities are unlocked gates, lack of intrusion detection and unrestricted access to buildings or premises (Reniers, 2017:38). Furthermore, vulnerability refers to the absence of security measures to protect valuable assets against risks like theft, robbery and burglary (Mahambane, 2017: 6).

1.8.9 Biometric technology

Biometric technology is a scientific recognition of people based on the features of their body using a computerised system to verify their identity (Ashbourn, 2014:14). According to Brackenridge (2014:14) this recognition relies on measurable physiological characteristics such as fingerprint, hand vein patterns, the retina, iris, facial expressions and behavioural characteristics such as voice recognition, signature verification, keystroke, gait analysis and body temperature to authorise their access into the premises. At the Mangaung Metropolitan Municipality, the only biometric system is fingerprint scanner which is installed at the Bram Fischer building, the head office and the Jubelium building.

1.8.10 Protection

Protection is defined as a process of securing physical and tangible assets from security risks. This is done through the application of the seven pillars of security namely physical; technical; human; information; communication; procedures and management (Cabric, 2015:3). The protection focuses on the value of what is protected, the probability and the impact of security breaches will inform the strategy to be selected from these seven pillars of security. Speed (2016:19) maintains that protection is a process of how organisations secure physical and tangible assets from risks through policies and procedures. The protection strategy adopted at the Mangaung Metropolitan Municipality includes physical security measures made up of gates, doors, turnstiles and burglars proofing; security personnel; policy and procedures; and a biometric system.

1.9 OUTLINE OF THE DISSERTATION

Chapter 1: Introduction and motivation for research

This chapter presents the introduction and motivation for the research. The study entails the evaluation of access control within the Mangaung Metropolitan Municipality's regional offices. The chapter provides the rationale for the study, the problem statement, aims and objectives, research questions, the value of the study, and key theoretical concepts, and the demarcation of the study.

Chapter 2: Research methodology

This chapter discusses the research methodology, approach, design and data collection methods, used to solicit information from the employees of the Mangaung

Metropolitan Municipality on their perceptions of the effectiveness of access control measures in the three regional offices. This chapter also addresses reliability and validity and ethical considerations.

Chapter 3 Literature review

This chapter entails a discussion of literature relevant to the study as written and reviewed by other authors. It provides discussion on the development of various access control models, measures, policies, and technology effective and relevant to safeguard property, assets, and the protection of life in organisations as well theoretical perspective of the study.

Chapter 4 Research Findings: Data Analysis and Interpretation

This chapter presents the research findings from data collected from the participants in the research process. It presents a discussion on the data analysis and of the interpretation of the findings of the study.

Chapter 5 Conclusion and Recommendations

This is the concluding chapter and presents recommendations to assist the Mangaung Metropolitan Municipality’s regional offices in effective access control measures to combat crime and for the protection of assets and property.

1.10 CONCLUSION

This chapter provides the orientation of and background to the study by defining important concepts. It outlines the problem statement, rationale, aims and objectives and the research questions that guided the study. Finally, it provides a layout of the chapters of this dissertation.

CHAPTER 2
RESEARCH METHODOLOGY AND DESIGN

2.1 INTRODUCTION

This study followed a phenomenological approach that relied on the collection of data based on the experiences and feelings of the research participants at a given situation under study (Creswell, 2018: 50). According to Pretorius (2012: 5) this method is appropriate for qualitative research because it is tailor-made for extracting information from the participants in protected and confidential settings.

2.2 RESEARCH APPROACH

The study followed a qualitative approach because it sought to obtain broad descriptions and detailed information about the research topic and answers to the research problem (Lekubu, 2015:8). Bairagi & Munot (2019:77) take this argument further by stating that qualitative research is a form of social enquiry that focuses on the way people interpret and make sense of their experiences and the world in which they live. In addition, qualitative research is a means for exploring and understanding the meaning individuals ascribe to a social or human problem. Muchengetwa (2019: n.p.). This approach enabled the researcher to use the perceptions, feelings and experiences of participants to understand the effectiveness of access control in the Mangaung Metropolitan Municipality‘s regional offices to restrict and control the movement of people in and out of the premises.

2.3 RESEARCH DESIGN

The research design is a plan or blue-print that can serve as a guide on how to conduct the research, which methods will be used to collect information, and what kind of data analysis will be used to answer the research questions (Muchengetwa, 2019: n.p.). The study followed a phenomenological approach as a method for qualitative research because of its suitability as a qualitative method to describe a phenomenon in whatever is being examined. To achieve this, the researcher used a qualitative research method to explore the behaviour, perceptions, feelings and opinions of participants in the regional offices in order to gain insight and knowledge about their perception of the effectiveness of access control. The reason for using this approach was the desire to fully understand participants' lived experiences of access control measures in the regional offices without focussing on the specific concepts (Creswell, 2018:258). The researcher used interviews to understand the meaning the participants placed on the phenomenon under study. In this context, the study sought to evaluate the adequacy and effectiveness of access control measures within the Mangaung Metropolitan Municipality' regional offices.

An in-depth literature review was conducted to obtain background knowledge about access control to orientate the researcher in the context of the topic of study.

2.4 DATA COLLECTION METHODS

Data collection methods are tools that the researcher uses to collect information from participants in the research process. According to (Mukherjee, 2020), the data collection mechanism plays an important role in all empirical research as a basic input for an understanding of a phenomenon under study (Mukherjee, 2020: n.p.)

The following data collection methods were used in the study:

2.4.1 Interviews

Queiros (2017:378) maintains that interviews are the most popular form of gathering data in qualitative research. The researcher used an interview schedule consisting of face to face unstructured interviews **(Annexure A)**. To test the practicality of the interview questions, the researcher conducted a pilot study with the three Regional General Managers at their respective regional offices. The interviews which lasted for thirty minutes per participant were conducted in their respective regional offices from 1 September 2020 until 30 November 2020. These consisted of open- ended questions, to explore the participants' perceptions, knowledge and experience of the effectiveness of the existing access control measures within Mangaung Metropolitan Municipality’s regional offices.

To record the data as accurately as possible, a tape recorder together with a notebook was used to record the responses of the participants and the researcher’s observations during site visits (Mason, 2002:62).

With an understanding that verbal communication is key to the collection of reliable and accurate data from the participants, the researcher chose interviews as the most suitable data collection method.

The reasons for using this method are:

(a)The researcher is in charge of the process of extracting information from the respondents. The researcher was able to probe for a deeper meaning of the responses of the participants and to ask for clarity where necessary; (b) Participants get a clear understanding of the questions that are asked by the researcher and an opportunity to request clarity in the event of uncertainty (c) The presence of the researcher ensures cooperation from the respondents which enhances their response rate (Cebekhulu, 2016: 2). This was done by establishing a rapport with the participants through the assurance of strict adherence principles of anonymity, confidentiality and right to privacy.

2.4.2 Literature Review

The aim of a literature review is to provide context for the research by showing where the research fits into the existing body of knowledge (Tabane, 2019: n.p.). To do this, the researcher conducted a literature review of the research topic to determine what has been in the public domain about the significant role that access control plays in protecting buildings, premises, and their inhabitants. For this purpose, the researcher consulted primary sources including both published and unpublished material relevant to access control. These include texts of law, newspaper reports, interview transcripts and official documents. In addition, secondary sources that included recently published books, journals and articles from both local and international different relevant to the study were consulted. The researcher also reviewed academic sources, especially those in Unisa’s institutional repository on previous dissertations and theses in the school of criminology and security science were consulted to gain insight on various aspects of physical security access control.

To broaden a deeper understanding of access control, the researcher incorporated the following pieces of legislation as promulgated by the South African Government for the implementation of access control both as a legal requirement for both public and private entities:

- The Trespass Act No 6 of 1959
- Control of Access to Public Premises and Vehicle Act 53 of 1985 as amended with reference to section and sub section 2.2(g) and finally
- The Minimum Information Security Standards document of 1996.

The provisions of these acts and policies required the Mangaung Metropolitan Municipality to implement integrated access control measures to its premises to safeguard its personnel, clients, stakeholder, properties, and business continuity processes

2.5 POPULATION AND SAMPLING

2.5.1 Target population

The target population in this study comprised of all employees of Mangaung Metropolitan Municipality currently employed at the three regional offices.

They were categorised as follows to give the researcher a clear picture of the composition of the target population for the study:

(a) The users of access control measures like employees.

(b) The implementers of access control who are private security officers and their supervisors from the different security companies contracted by the municipality.

(c) Regional general managers assigned to each region to monitor and oversee compliance with the service level agreement between the municipality and the contracted security companies with specific reference to access control measures.

In this way, the researcher collected data, and generalised the respondents' perceptions, feelings and experiences on the effectiveness of access control in their working environment (McCombe,2019:np).

2.5.2 Sampling procedure

The study was conducted on a sample of the population in three regional offices within the metropolitan municipality. It excluded employees employed at the satellite offices and other various plants of the municipality. As it was impossible to involve all members of the population in the study, the researcher drew a sample from this population to draw conclusions about the study (Cherry, 2018:np). To do this, the researcher obtained statistics on the total number of employees at the Mangaung Metropolitan Municipality's regional offices from the human resources department. After receiving the list, the researcher purposefully selected the participants to form a sample for each regional office, based on the researcher's judgement of participants' knowledge and experience in the operation of access control in respective regional offices (Fouche, 2021:382).

The researcher selected a total of 45 employees which is fifteen per cent (15%) of the total number of employees of the regional offices which constituted a sample for the study. From a total of one hundred and seventy (170) employees in the Bloemfontein regional office, twenty (20) were selected to participate in the study. From 55 employees in the Thaba Nchu regional office, ten (10) were selected and fifteen (15) from one hundred and twenty (120) in the Botshabelo regional office were also selected.

2.6 DATA ANALYSIS

Data analysis entailed the analysis and interpretation of information obtained by the researcher from the research participants (Zhang, 2016:2). According to Taole (2019: n.p.), a qualitative data analysis is divided into four broad categories: (i) organising and arranging data; (ii) exploring data, -pulling apart, –discovery and coding; (iii) interpreting and reflecting; (iv) integrating and writing. The researcher acquainted himself with the data by repeatedly reading the interview reports collected. Secondly, the researcher generated themes, categories and patterns to determine common denominators from the perspectives and reflections of the participants (Minnaar, 2017:142). According to Creswell (2016:175) themes are the major findings in a qualitative study because they present evidence of the central phenomena of the study. In this study themes were identified according to the participants' perceptions of access control systems. One of the advantages of using themes is that they are useful in examining the perspectives of different research participants by highlighting similarities and differences to generate unexpected insight (Taole, 2019: n.p.).

The researcher used a spiral data analysis method in which data was arranged and organized into manageable segments using index cards, folders, tables and graphs, and those were broken down into stories and sentences of the exact words of the participants (Zhang, 2016:2). In addition, data was perused repeatedly to enable the researcher to get a clear understanding of the responses of the participants to develop categories and interpretations. During the data collection phase the researcher wrote comments in the margins to capture participants' comments accurately.

The researcher furthermore coded the data for different paragraphs, lines and sentences from hard copies of the interview. An Excel spreadsheet was used to organise data collected from open-ended questions to highlight what the participants were saying about each question. A journal and field notes were used as primary ways of capturing data. The interview schedule was read through and notes were written in a field journal for general ideas that have been brought forward (Minnaar, 2017:142). The results were presented in a narrative form and supported by direct quotations from the raw data. The data was then transcribed and placed into categories and this was followed by the interpretation of data (Minnaar, 2017:142).

2.7 MEASURES TO ENSURE TRUSTWORTHINESS

Trustworthiness in qualitative research is defined as the believability of the research findings. Polit (2014: n.p.) maintains that the trustworthiness of a study in qualitative research refers to the degree of confidence in the data interpretation and methods used to ensure the credibility and quality of the study. Mudondo (2021:121) proposed the following four criteria that the researchers need to follow in dealing with trustworthiness:

Credibility: Credibility is defined as the ability of the data collection tools to reflect on the responses of the participants in line with the phenomenon under study (Mudondo ,2021:124). The researcher collected data from various sources such as open - source documents like legislation and reports on various aspects of access control. Furthermore, a literature review was conducted to obtain corroborating evidence to such findings of the data analysis. Thirdly, the researcher used triangulation by using more than one source of data or multiple approaches to analyse data in order to enhance credibility. This was done by combining information gathered from the face – to - face interviews conducted in conjunction with the researcher's observation of the operation of access control measures at the regional offices (Mudondo ,2021:124).

Confirmability: Confirmability is defined as the avoidance of bias in the research process (Mudondo ,2021:134). The researcher ensured objectivity by examining the data collected and making efforts to avoid any pre-conceived ideas that might compromise the integrity of the data collected for interpretation purposes (Minnaar, 2017: 144). The researcher also ensured that he did not in any way influence the outcomes of the study with his knowledge of access control, but articulated the feelings and experiences as expressed by the participants in the study (Maxfield& Babbie, 1995:208).

Transferability: This is defined as the extent to which the results of qualitative research can be transferred to other research situations. The researcher provided a description of the participants and the research process to ensure transferability judgement by other researchers interested in the study (Korstjens, 2018: n.p.). Furthermore, the researcher provided an opportunity for interested parties with evidence that the research study could apply to other contexts, situations, times and populations. This proved that, the findings can be transferred to other contexts.

Dependability: This refers to the stability and aspects of consistency of research findings (Korstjens, 2018: n.p.). In achieving this, the researcher checked and ensured that the analysis process conformed to an acceptable standard of a research design. The researcher further made use of credible sources such as Sabinet to ensure that the research findings are based on credible sources. Thirdly, the researcher maintained audit trails by keeping a complete record of the research process and keeping documents for cross checking and keeping information for the study as raw data documents (Korstjens, 2018: n.p.).

2.8 ETHICAL CONSIDERATION

Ethical consideration refers to adherence to the moral principles and values in the research process to ensure the protection of participants (Thoka, 2021:13). Ethical principles are important to guide the researchers to observe moral principles, behaviour and conduct that will not be harmful and prejudicial to the participants during the data collection process (Fouche 2012:117). The researcher was granted ethical clearance by the University of South Africa to conduct this research in the three regional offices of the Mangaung Metropolitan Municipality **(Annexure B).** The following ethical considerations were adhered in line with UNISA’s Code of Ethics for Research in the College of Law:

2.8.1 Institutional approval

Permission for approval to undertake research in Mangaung Metropolitan Municipality’s regional offices was sought from the City Manager with a commitment to keep information solicited confidential for the research process **(Annexure C**) This was extended to the owners of private security providers contracted to provide security within the regional officers seeking permission to include their security officers and managers in the study**.**

2.8.2 Informed consent

For the research to be regarded as credible, participants have to agree to take part in the study without any undue pressure. The researcher ensured that participants were not coerced into participating in the research process. The participants were provided with an informed consent form **(Annexure F)** containing information about the goals, aims, objectives and the purpose of the research, the type of interview and other data collection procedures with the participants as well as the risks and benefits involved in the research process (Maxfield & Babbie, 1995: 161).

The participants were encouraged to sign a statement giving them informed consent and willingness to take part in the study and to confirm their knowledge of the process and procedures to be followed during the research process (Blair, 2016:57).

2.8.3 Voluntary Participation

Babbie (2008:438) maintains that participation in a research process needs to be voluntary with every effort made to assure the target population that this process is not compulsory.

The researcher assured the participants that their participation was voluntary and that they were not compelled to participate and could withdraw at any given time if they so wish, without any consequences.

2.8.4 Anonymity and the right to privacy

Anonymity refers to the concealment and withholding of the personal information of the participants in the study to prevent any recognition by others (Fouche, 2021:124). On the other hand, the right to privacy refers to the secure physical setting from which data is collected (Fouche, 2012:124). The researcher adhered to the principle of anonymity and the right to privacy of participants. The identity of the participants as well as the Mangaung metropolitan regional offices at which they were employed were concealed. Nick- names in the form of numbers were allocated to each participant using an abbreviation to indicate the region from which interviews were conducted (Denscombe, 2002:180).

2.8.5 Confidentiality

Confidentiality refers to keeping the private information of research participants secret and being divulged to a third party without the consent of the participants

(Fouche, 2021:124). The researcher maintained strict confidentiality of data collected from the participants by ensuring that it would neither be publicised nor would be disclosed to third parties without the approval of the participants. The names of the participants, together with their regional offices were removed from data, collection forms and replaced with acronyms. This was followed by creating a master file containing details of the participants that was put in a locked safe (Maxfield & Babbie, 1995:155).

2.8.6 An atmosphere of trust

The researcher created an atmosphere of trust in which participants were guaranteed respect and protected from any embarrassment and stress related situation (Babbie, 2001:522). This was done by making an undertaking to the participants that their participation was solely to provide answers to the research question of the study and their identity and responses will remain confidential.

2.8.7 Avoidance of physical harm

The protection of participants from any physical harm is important from an ethical standpoint in the research process, to ensure that they are not exposed to situations that might lead to both mental and physical harm (Arifin,2018:30). Precautionary measures were taken to ensure that all the participants were protected from any physical harm that might arise as a result of exposure to injury and health matters during the research process. The researcher was sensitive to participants' emotions when probing questions that could psychologically harm them (Arifin,2018:30). The researcher further protected the participants by avoiding any behaviour that might embarrass, frighten, offend or harm them.

2.8.8 Protection of information

The protection of information is important from an ethical point of view in the research process because it confirms the integrity of the research process. This is done by ensuring that information is not modified, manipulated, divulged or, used for any other purpose other than the intended one. Personal information was collected in terms of the Protection of Personal Information Act 4 of 2013 that guarantees participants' information will not be used against them (Govender, 2018: n.p).

2.8.9 Academic integrity

According to UNISA's research policy, academic integrity is defined as a policy guiding research and development by maintaining human dignity, honesty, trust and fairness in all teaching and research activities to prevent plagiarism, cheating, falsification and fabrication. The researcher strived to demonstrate a high degree of honesty with professional colleagues by ensuring that all sources consulted were properly acknowledged to avoid academic cheating and plagiarism (Mudondo ,2021:12).

The researcher conducted this study with great honesty and integrity by being authentic to the participants through avoiding misleading them to secure their cooperation in the research process. In the event this was unconsciously done, every effort was made to ensure that participants were debriefed at the end of the session about the unfolding of events to maintain their integrity during their departure (Denscombe, 2002: 178).

2.9 DEMARCATION OF STUDY

Griffiths (2020: np) maintain that the demarcation of a research project is a process of setting boundaries that determine the scope of the study. Setting the boundaries will entail what the researcher is not going to do other than what is stated in the research problem (Griffiths (2020: np).

The study was demarcated with regard to time span and place. The study was conducted at the three regional offices of the Mangaung Metropolitan Municipality that are situated in Bloemfontein, Botshabelo and Thaba Nchu, and excluded the satellite offices and various plants falling under these regional offices. Furthermore, the state focussed on the losses due to security breaches related to access control from 2011 to 2018.

2.10 CONCLUSION

This chapter provides a discussion of the research strategy implemented outlining the research methodology, approach and design that the researcher followed in this study. Included in this discussion were the identification of the target population, the sampling procedure, data collection and analysis methods, trustworthiness and ethical considerations which were concluded with the demarcation of the study.

CHAPTER 3
LITERATURE REVIEW

3.1 INTRODUCTION

The focus of this study relates to access control in physical security at the Mangaung Metropolitan Municipality regional offices which has not been explored by empirical research. Until the 9/11 terrorist attack in the United States of America, this phenomenon had hardly been explored by organisations throughout the world (Fenandez, 2007:260). This incident stimulated a need around the globe to control and regulate access to restricted areas such as ports of entry, government buildings and other critical infrastructure. Much interest in access control was stimulated in the research community by recognising that access control to physical property and information have many features in common to authenticate and identify an individual's access to premises and computer software (Fernandez, 2007:260. Therefore, managing and controlling physical access to facilities and buildings is a critical aspect of a good security program (Baker, 2016:97).

Access control security measures relate to a system used to ensure that access to premises, buildings or rooms is restricted to only authorised, people, whereas those likely to pose a threat to organisational assets, property, employees and visitors are denied permission and authorisation to enter premises (Baker,2016: 98). The main purpose of an access control system is to monitor the location of individuals within a building, to control areas where individuals can gain access, and to manage access permissions in the organisation through a proper process of identification and authentication (Baker, 2016: 98).

In this chapter, the researcher will discuss the development of access control models and, access control measures, policies and aids effective and relevant to safeguard property, assets and protection of lives in organisations. In addition, the researcher will provide a broader overview of access control in the context of physical security as a tool to grant or deny access to buildings and premises and provide an overview of access control measures at Mangaung Metropolitan Municipality.

3.2 DEFINITION OF ACCESS CONTROL

Access control is a security system designed to regulate and restrict the entrance of people and vehicles into a facility by granting access to authorised people and denying access to unauthorised people to the premises of the organisation (Lombard, 2013:42). In its basic sense, access control means the selective restriction of access to a place, premise and property subject to identification, authentication and authorisation (Lombard, 2013:42). Pieterse (2017: n.p.) regards it as the first line of defence that provides the organisations with an extra layer of security and protection for their premises

According to Saflec (2017) access control is a security measure that regulates the movement of people in, within and out of premises and buildings by requiring identification and monitoring, documenting, and recording their credentials (Saflec, 2017:1). Brackenridge (2014:14) extends this definition and regards access control as the selective restriction of individual access to a place, building, resource or installation based on the verification of their identity before being given permission and authorisation to enter a building, premise and restricted areas. Access control is, therefore, an element of physical security to ensure the protection of premises and their assets (British Security Industry Association, 2016:14).

In its basic sense, access control aims to prevent the occurrence of security breaches and this is done by monitoring and regulating the movement of people in and out of facility, and by allowing those permitted entrance and denying entrance to unauthorised people. Common among measures to realise this are physical barriers like, fences, gates, locks and keys; electronic access control measures such as biometric systems; magnetic cards; ID cards and badges (Marazos, 2013:676).

Based on the above, access control contributes significantly to the protection of organisational property and resources. The effective implementation entails restricting the movement of people in a facility, controlling entrance to buildings and offices, and allowing only authorised people to the premises while those posing a threat are prevented.

3.3 DEVELOPMENT OF ACCESS CONTROL SYSTEM

The application of strong access control measures was originally implemented by military organizations to control, regulate and monitor the movement of people in and out of their bases (Erbschloc, 2017:164.). This became common practice when adopted by governments and other agencies during World War 11 and throughout the Cold War era. During the age of terrorism especially the 9/11 attack of the USA, countries across the globe saw the need to intensify access control access measures in their critical infrastructures by implementing integrated physical access control measures using among others strategies such as: secure areas of buildings and facilities; zoning of areas within the buildings; secure storage devices such as vaults, safes and lockable cabinets and finally, mitigating insider damage through to the application of ID management and surveillance technology (Erbschloc, 2017:164.).

The implementation of access control by the business community started in the early 1960s as a security measure to prevent the utilisation of missing keys, including the trouble of replacing those keys not returned by former employees who left the organizations due to various reasons (Securecomm Technologies, 2014: n.p.). With the progression of time, access control to premises underwent some developments with the application of locks and keys being used to control access measures which were further integrated with advance electronic equipment (Securecomm Technologies 2014: n.p.).

As technology evolved one of the earliest devices, the simple keypad was introduced (Houlis, 2020: n.p.). It used personal identification numbers (PIN) that matched data in an electronic device to grant access to a facility and secure zones (Houlis, 2020: n.p.). In the 1980s, swipe technology improved the use of locks and keys and magnetic striped cards that were read against the card readers using Wiegand technology. The term ‘Wiegand’ refers to the technology used in card readers and sensors. The system is a wired communication interface that operates between a reader and a controller. Typically, Wiegand technology is found in cards, fingerprint readers, or any other data- capturing devices (SecurityInfoWatch.com, 2017: n.p.).

With the introduction of biometric systems, access control became regulated by using both physiological and biological traits in the authentication of people's identities (SecurityInfoWatch.com, 2017: n.p.). Thus, access control emerged as an updated and effective method to ensure that access to a facility is restricted and regulated by using sophisticated techniques, by providing security against methods used by criminals to breach, pick or copy keys and locks to gain access to property. Although security systems exist at the Mangaung Metropolitan Municipality, this study seeks to examine the effectiveness of such measures with a specific focus on access control measures.

3.4 TYPES OF ACCESS CONTROL SYSTEMS

Various types of access control measures are used by organisations to restrict and regulate the movement of people in and out of the buildings and premises. Dingle (2015: 97) maintains that there are four fundamental systems for access control used in premises and buildings. These are (i) personal recognition of people by someone entrusted to operate access control at the premises; (ii) unique knowledge of something such as a pin or code and password; (iii) unique possession of a token issued to the user like a key, card or ID badge, and lastly, (iv) biometric systems that identify the user by comparing individual details with information stored in a data base (Dingle, 2015:97).

Harris (2016) suggests that an access control system usually entails physical access control system that uses security barriers like fences, locks, gates, manhole, mantraps and turnstiles; secondly, technical systems which uses surveillance devices like CCTV and alarms and lastly; an administrative system that involves policies and procedures to manage access control in the organisation (Harris, 2016:29). The justified implementation of access control in an organisation depends on two fundamental circumstances. Firstly, an area that must be controlled and regulated, secondly, a list of people who need to enter the facility, buildings and premises at given times (Truett, 2015: 87). Others such as, Croner-i limited (2020) maintain that the fundamental requirements for access control rely on three principal components. The first is a perimeter in which all access points are secured and controlled; a portal to control access through barriers and lastly, a means of identification and authentication (Croner-i limited 2020: n.p.).

3.5 ELEMENTS OF ACCESS CONTROL

Access control measures in buildings and facilities are usually made up of three elements (Lombard 2013: 38). It starts with pre- access control where the suitability of a person is determined through using surveillance methods like closed-circuit television and security guards, before being granted access into a facility and premises; secondly, granting access, which is the actual process of granting or denying entry of people into the premises and buildings subject to the identification and authentication of their credentials. Lastly, a post- access control, which is normally referred to as egress control, operated at exit points to monitor the activities of people leaving the premises and to prevent the unlawful removal of property and assets (Lombard, 2013:38).

In addition to these, the Department of Homeland security in the United States of America (2015) concur that access control is made up of four elements; inter alia: security barriers, authentication devices, a panel to operate the barriers and finally surveillance devices to detect intrusion (American Homeland Security, 2015:1).

3.6 PRINCIPLES OF ACCESS CONTROL

The implementation of access control to regulate and restrict entry and exit into and out of premises and facilities, is guided by three security principles (Esfand & Sabbari, 2014:153). The first principle is the authentication process which entails the verification of the identity of a person by using their credentials stored in a data base such as a personal identification number (PIN), biometrics and passwords. The second principle is the authorisation process which ensures that access is granted only to people who are entitled to be on the premises and the third principle is accountability, which uses audit trails to ensure that authorised people are accountable to their actions during their presence at the facility. Lastly, the privacy principle to protect the identity of individuals is applied to ensure the protection of the confidentiality of the information of users of the system (Esfand & Sabbari, 2014:153).

Moses (2016: 669) expands further on these principles of access control by adding another two principles that include the identification process which uses the usernames, user identity numbers (IDs) and account numbers. Finally, the auditing process to monitor the effectiveness of the access control system by maintaining an audit trail that keeps a record of all previous access movements and activities within the premises (Moses ,2016: 669). These principles are important in access control to ensure that organisations properly identify people before giving permission to enter premises and that their records are kept for future reference.

Based on the above, access control plays a significant role in regulating the movement of people in and out of premises through ascertaining their identities before authorisation is granted; or denied, allowing them into buildings and properties.

3.7 OBJECTIVES OF ACCESS CONTROL

Access control programs are instituted by organisations to permit or deny entry to any given space in order to control the movement in, from and within the premises (Homeland Security, 2015:1). Its main objectives are to protect employees, visitors, property and assets from unauthorised people. Therefore, the goal of effective access control is threefold, namely: (a) to allow entry only to people designated by management to be into the premises; (b) to alert security guards in the event of intrusions and other security breaches; and lastly, (c) to minimise the opportunity to commit a crime, by preventing access and restricting it to authorised people only to assets, computer equipment, operating procedures, and other sensitive materials (Baker, 2016:98).

The Department of Homeland Security in the United States of America identified the following three objectives of access control: (a) to allow or refuse permission of people to enter or leave the premises subject to verification of their identities and particulars ,(b) To search people entering the premises in order to ensure that they are not carrying dangerous weapons that can endanger the lives of employees and members of the public and lastly, (c) to document the particulars of all people entering and leaving the premises to be able to follow up in the event of security breaches occurring in the premises (Homeland Security ,2015:1).

These objectives are relevant to the regional offices of the Mangaung Metropolitan Municipality to ensure that the regional offices implement an effective access control system that will not only protect the employees, but also members of the public who are entitled to be on the premises.

3.8 THE ROLE OF ACCESS CONTROL

Access control plays an important role in maintaining physical security. It allows only the authorised entry of people and vehicles onto premises and restricts entry of those not granted permission. Moore (2020) maintains that access control enables organisations to secure their facilities and assets by effectively managing access requests based on individual identity and an organisational access control policy (Moore, 2020: n.p.). Therefore, the role of access control in organisations is to detect security breaches and to prevent any unauthorised entry onto premises, to prevent criminal activity such as theft, vandalism, burglary, and arson (Moore, 2020: n.p.). Access control measures provide protection against any physical harm and injuries to employees and other lawful stakeholders within the premises. It provides a detailed electronic visitor history and record through a paper trail that can be inspected, to track occurrences within the facilities in the event of security breaches that might lead to the loss of life, damage to property and unauthorised removal of organisational assets (Saflec, 2018:1).

Given the above, the role of access control at Mangaung Metropolitan Municipality is an important security measure to control and record the movement of people in and out of the premises. In this way, access control measures serve the purpose of safeguarding organisational assets and protects employees and visitors. More details are provided in Sections 3.12.1.2.

3.9 INTERNATIONAL STUDIES IN ACCESS CONTROL

Across the globe, access control systems are being implemented to restrict and control access to facilities and premises by ensuring that only authorised people enter the premises of organisations. The need to protect assets in buildings and to control access to restricted areas such as airports, naval ports or government buildings has created much interest in the research community (Fenandez, 2007:260).

Market trends indicate that the global access control market is expected to reach 13.55 USD billion by the year 2025. The analysis of this market was regionally segmented into thirty countries such as North America, Europe; the Asia-Pacific region; the Middle East, South Africa and the rest of Africa (Avinash, 2020: n.p.). The US emerged as dominating this market with 2.47 USD billion in 2017 due to the constant threats of their crime rates, cyber and terrorist attacks. The Asia-Pacific region which includes China, Japan and India, is experiencing growth in this market as a result of increasing industrialisation and commercialisation that requires more security (Avinash, 2020: n.p.).

The other analysis was the vertical segmentation of the market into commercial, government and residential segments. The results showed that the commercial segment dominated the market with 26.90% due to the requirement for access control to protect people and assets against unauthorised access.

During an online global survey conducted in 2016 with 50000 ASIS (American Society for Industrial Security) members and customers on the effectiveness of physical security, participants in the study confirmed that installing perimeter protection and access control systems to secure high-value assets are a fundamental responsibility of security departments. The results confirmed the following measures to control access: photo identification badges at eighty per cent (80%) and parking or gate control at sixty per cent (61%) (ASIS International, 2016:56).

In another study among security directors, managers and consultants conducted by ASIS International, the results indicated that thirty-four per cent (34%) of the security directors felt that access control systems assist the organisation’s security in limiting security breaches like burglary, theft, and damage to property. A slightly smaller percentage (28%) of the respondents indicated that integrating physical and logical access control would have the most impact on improving the organisation‘s overall access control system. From this study, it can be deduced that the role of access control in minimising organisational losses and the protection of its employees and stakeholders cannot be overemphasised. To be effective, access control needs to be integrated with both physical and technological measures (ASIS International, 2016:56).

The results of a study conducted among fifty-six (56) organisations, drawn from five major sectors in Ghana in 2018, that focused on the following four areas of access control application such as (a) access control policy, (b) user access management, (c) user responsibility and (d) accountability, showed that the 66% implementation rate of access control in the organisations surveyed was not effective. Furthermore, there were inconsistencies in the implementation of access control with financial institutions and health-care institutions outperforming educational and government services (Yaokumah, 2018: n.p.). Another study was conducted by the Victorian Auditor-General in Australia on the safety of government buildings due to threats of security breaches in these buildings, which affected the safety of employees and clients (Greaves, 2019: n.p.). A sample involved two government departments namely Health and Human Science and the Department of Justice and Community Safety. The focus of the study was to assess whether current security measures in these buildings were effective in preventing unauthorised entry and anti-social behaviour. To do this, covert tests were conducted on access control and security culture in these buildings. The study found that weaknesses in staff culture and physical security procedures rendered physical security measures ineffective against unauthorised entry into the buildings. One of the recommendations was that employees must be trained on security measures to enable them to identify and report suspicious behaviour at access control points (Greaves, 2019: n.p.).

Chapa (2019: n.p.) maintained that the 9/11 terror attack in the United States prompted the US government to intensify access control measures in all federal buildings by issuing employees and contractors with identity cards for verification purposes, based on their level of security clearance (Chapa, 2019: n.p.).

What can be learnt from these developments is a clear indication that organisations are starting to implement access control measures that are integrated with technology. Yaokumah (2018) however, maintains that there are inconsistencies in the implementation of access control in some countries due to political systems, legislation, social and economic conditions, and organisational culture (Yaokumah, 2018: n.p.). Nevertheless, the importance of access control for facilities to reduce the vulnerabilities of organisations and to protect their employees and property cannot be overemphasised.

3.10 LEGISLATION AND ACCESS CONTROL SYSTEMS IN SOUTH AFRICA

The safeguarding of state properties, assets and personnel is an important contribution in ensuring the safety and reducing the loss of state assets (Department of Public Works, Integrated Security Policy,2013:2). In South Africa, this responsibility lies with the accounting officers of different government departments per provisions of the South African Constitution Act 108, 1996, as well as the Public Finance Management Act of 1999 as amended (Department of Public Works, Integrated Security Policy, 2013:2). The implementation of effective access control measures in both South African public and private premises is derived from a series of legislation that were promulgated by the South African government including the primary legislation which is the Trespass Act No 6 of 1959. The purpose of this act was to prohibit unlawful entry or presence on land and buildings by giving the owner the authority to deny or evict such persons under certain circumstances. In other words, this act prohibits people who are not authorised to enter premises without permission being granted to them through reservations of their granted entry (Trespass Act 6: 1959, section 1).

The application of this act empowers an authorised person to remove any person from premises if there is a reason to believe that permission was not granted for him/her to be on the premises. It furthermore affects their removal if it is in the interest of safeguarding the premises, assets and people therein (Kole, 2014:122). Therefore, trespassing on premises by unauthorised people should be prevented through the application of access control procedures that entail elements in a policy such as “trespassers shall be prosecuted” (Kole, 2014:122).

Another important piece of legislation governing access control in both the public and the private sector is the Control of Access to Public Premises and Vehicles Act 53 of 1985 (as amended). The purpose of this act is to provide for a comprehensive access control system at public premises and buildings by monitoring the movement of people, vehicles and materials into, within and out of the premises (Control of Access to Public Premises and Vehicle Act 53: 1985, Section 2). According to Subsections 2.2 of the act, it places an obligation on the heads of departments and institutions to apply access control by ensuring that any person gaining access to their premises is safe, has a valid reason to enter, is authorised and that employees and members of the public, including contractors and stakeholders, are not exposed to any danger as a result of security breaches. Furthermore, all government departments are required to institute measures to control access and the movement of employees, visitors and contractors through proper verification of their details. The heads of departments are also empowered to designate personnel like security officers to act as authorised officers in implementing access control at the premises (Control of Access to Public Premises and Vehicle Act 53:1985, section 2).

In terms of Subsection 2.2 (g) of the above-mentioned act, heads of institutions are entitled to conduct searches on everyone entering and exiting the premises. In addition, the act allows them to recover any property of the organisation and confiscate any object that might endanger the lives of the occupants of the building, visitors, contractors and stakeholders. Therefore, all vehicles both private and government-owned, must be searched when entering and leaving premises, to ensure that there is no unauthorised removal of assets and property (Control of Access to Public Premises and Vehicle Act 53: 1985).

A study conducted by the Institute of Security Studies on the perception of employees regarding the effectiveness of security measures implemented to prevent theft from mine premises, Coetzee, and Horn (2007:53) found that most participants cited effective surveillance, effective access control, effective perimeter fencing and security guards as effective measures to regulate access control, to curb theft in the mines. In another study conducted on safety and security measures at secondary schools in Tshwane, Van Jaarsveld (2011) found that scholars and teachers felt that there were ineffective access control measures. Twenty per cent (20%) of the participants indicated that there was security at the gates and that they were left open. This created a situation that allowed scholars and visitors to enter and exit the premises at any time without being monitored. This study also confirmed that ten per cent (10.1%) felt that there were not enough guards at exit and entrance points. It was furthermore revealed that eighty-four point nine per cent (84.9%) of the learners did not make use of identity cards (Van Jaarsveld, 2011:116).

To prevent unauthorised entry into premises, Kole (2013) proposes the following visitor control system: A person requiring permission should produce an ID document or drivers' licence, the person is provided with a visitor's badge and there are daily escorts for visitors and contractors within the premises. The act makes it very clear that a person convicted of violating the Control of Access to Public Premises and Vehicle Act 53 of 1985)" shall be liable to a fine not exceeding R2000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment' (Control of Access to Public Premises and Vehicle Act 53 of, 1985: 6). These provisions also apply to the Mangaung Metropolitan Municipality which is required to implement integrated access control measures at its premises and offices and to safeguard its personnel, clients, stakeholders, properties, business continuity and processes.

3.11 ACCESS CONTROL METHODOLOGY

The operation of access control in buildings and premises is informed by various methodologies, depending on what is to be protected and the needs of the organisation. Access control methodology is an approach that provides a basis for access control rules and policies (Karimi, 2017:44). There are two types of access control methods to ensure the restriction of individuals within premises, according to Saflec (2018), the first one is logical access control security measures that restrict access to intangible assets like computer connections and data and system files. The second refers to physical control security measures that are implemented to restrict access to tangible assets like buildings and premises which is the focus of this study (Saflec, 2018:1)

According to Atlam (2017:253), access control methods are implemented at three levels, consisting of the following five factors: (a) the users of the system, (b) objects that need to be accessed by subjects, (c) actions seeking access through the authentication process, (d) privileges granted through authorisation and permission and lastly, (e) access policies that contain a set of rules governing access control in a facility (Atlam, 2017:253)

A brief discussion of the two methods of access control i.e logical and physical is provided in the next subsection.

3.11.1 Logical Access Control

The logical access control methodology centres on identification protocols that deal with computer networks and software to regulate and restrict access to information, objects and services through a computerised information system (Harris, 2013:11). This methodology is based on a three-legged principle known as confidentiality, integrity and availability (CIA) which is a model essential in guiding policies for information security within an organisation that must not be disclosed, altered and always available on a need-to-know basis (Harris, 2013:11). The logical access control method consists of the following three broad distinct models.

3.11.1.1 Role-Based Access Control (RBAC)

Conrad, Misenar and Feldman (2012: n.p.) state that role-based access control is a type of nondiscretionary access control method in the sense that the system users do not have any discretion about what they can access or transfer to another person. The role-based access control model is also known as rule-based access control in which access on a system is based and restricted to the role of the individual within the organisation as assigned by the system administrator (Conrad et al., 2012: n.p.). TED systems (2018:1) maintains that this is also based on the job responsibilities as contained in the job titles of individuals within an organisation.

The role-based access control (RBAC) model consists of three elements such as the user who is requesting access and roles, which are a collection of permissions and operations that are actions to the target resource (Bijon, 2013:462). Rath (2015) identifies the following guidelines of role-based access control as cited by the National Institute of Standards and Technology (NIST):

- The granting of access permissions and rights in the premises should be based solely on the roles and responsibilities assigned to an individual and his/her identity should not determine their assigned responsibilities in the granting access of in the organisation.
- Only permitted access control duties and responsibilities should be performed by individuals; to perform only the duties and activities which they're permitted to execute.
- Individuals should perform only authorised activities (Rath, 2015:24).

Considering the above, a role-based access control methodology is important in the implementation of access control whereby, without the above requirements, unauthorised people would not be permitted access to the premises and resources of the organisation.

3.11.1.2 Mandatory Access Control (MAC)

The mandatory access control model is commonly used in military institutions to implement access control under the classification policy of the organisation which sets parameters for the authorised and restricted access rights within an organisation (Antron Security,2021:np). Individuals are provided with labels that give them access to the facility in line with their security clearance (TED systems, 2018:2). Rao (2016:69). identifies four forms of this security classification: top secret, secret, confidential and unclassified and this system is mostly applied in tight security environments like government departments using a security classification such as top secret, secret, confidential and unclassified (Rao, 2016:69).

Antron Security(2021:np) maintains that one form of implementing the mandatory access control is a rule-based access control system in which all access rights are granted through a reference to the security clearance of the subject and the security label of the object to be accessed. Ekran Security (2020: n.p.) maintains that in a mandatory access control model, the security policy is managed by the security policy administrator where the user cannot override it to manipulate and access data illegitimately.

3.11.1.3 Discretionary Access Control (DAC)

Discretionary access control uses the identity of a person to decide whether to grant or reject an access request. The owner of the building defines which subjects can access the object with full access given to individuals with discretion by the owner of the facility in a specific location, physically and digitally (Harris, 2013:9). This is a need-to-know access model that restricts information and knowledge to selected people based on trust in them by the owner, in which access privileges to individuals ae based upon their credentials such as identification cards with the bearer's name and photo. It provides a flexible environment to access resources (Rao, 2016:70). Chapple (2004:30) contends that the implementation of the discretionary access control measure is based on the following two variables namely, the identity of the individual in which access decisions rely on the user's identity or group membership. The second is a type of access control list that allows a combination of objects and subjects access to a specific area.

3.11.2 Physical access control

Physical access control entails the security measures used to regulate and restrict the movement of people in and out of buildings and premises in order to protect assets, premises, employees and visitors (Alexandrou, 2018:1). Physical access control, therefore, refers to the utilisation of physical devices such as ID cards and badges, gates, fences, closed-circuit television (CCTV), alarms and proximity cards that rely on the authentication process involving the identification and verification of individuals access to the premises (Clutton, 2018:np).

The physical access control methodology begins with access control outside the facility's perimeter, used mainly to control the movement and access of vehicles and pedestrians near a point of entry (Homeland security, 2016:2). This is important since physical access control measures are instrumental in controlling access to specific areas within a facility and building by allowing some people in and keeping others out (Rao, 2014:5).

3.12 CATEGORIES OF ACCESS CONTROL

Three categories of access control measures are implemented to restrict entry and movement within and out of the premises and buildings (Harris, 2013:27). The first category involves physical access control measures that restrict access to the perimeter and buildings through physical devices like guards, fences, locks and gates. The second category includes administrative access control measures which entail policies, procedures and regulations and lastly, technical access control measures that are used for logical access control which deals with the computer network and software in information security to restrict access to firewalls, routers and encryption. Other categories include the functionality of the system after disruption, deterrence of unauthorised activities and finally, to compensate for additional security measures as needed (Harris, 2013:27).

3.12.1 Physical access control measures

Physical access control measures entail the application of barriers to monitor, control and manage access control within the premises. These measures are necessary to detect and prevent access from unauthorised individuals within the premises (Hutter, 2016:1). According to Alexandrou (2018), these measures are used to control entry and access to building areas by unauthorised employees or contractors and to prevent the unauthorised removal of organisational assets such as material and information (Alexandrou, 2018: n.p.).

A study conducted by Tlape (2019) that investigated the effectiveness of the access control system at Sol Plaatjie University in Kimberley, Northern Cape, found that access control was not effective due to the following challenges experienced in the implementation of access control: A lack of standardisation, resulting in the application of access control measures not keeping pace with the latest innovations; response to changing threat levels and also visitors to the organisation posing a challenge in respect of the management of access control (Tlape, 2019:76). In the same study, 34.4% of the participants indicated that the introduction of a fingerprint biometric system would improve access control, 22.2% indicated the use of student

ID cards to be introduced for access and 25.6% indicated that more security personnel should be hired to control and manage access control (Tlape, 2019:76).

Another study was conducted by Thoka (2021) to evaluate security threats and vulnerabilities at the Medupi power station which is situated at the Lephalale municipality jurisdictional area in Limpopo. Eighteen participants were purposively selected to participate in the study. The study found that access control measures were breached by criminals cutting the perimeter fence to gain entry into the facility undetected, especially if not monitored. The other weakness identified, was the presence of more than one entrance into the facility which gave easy access to unauthorised people into the plant (Thoka,2021: 96). To improve this situation, the study recommended the reduction of the number of entrance points into one in order to ensure effective monitoring, control and regulation of the movement of people in and out of the facility. Secondly, due to budgetary constraints which impacted on the effective implementation of access control measures, more resources to be made available for the improvement of access control measures (Thoka, 2021:100). The lessons learned from this study is that access control in critical infrastructure is important to regulate, monitor and control the entrance and exiting of people at the premises. This is applicable to the Mangaung metropolitan municipality which owns Centlec, an electricity distribution facility together with other critical plants such as water treatment, sewerage and reticulation system, council chamber etc.

3.12.1.1 Fences

Fences provide a boundary between public spaces and the perimeter of a building (Hutter, 2016:2). According to ASIS International (2009), the following types of fences are used to protect facilities and control access to premises: electrical, concrete, and barbed wire fences that are combined with an intruder alarm system and (CCTV) closed-circuit television (ASIS International, 2009:12). Two of the three regional offices of Mangaung Metropolitan Municipality such as Botshabelo and Thaba Nchu are protected by ordinary wire fences except for the Bloemfontein regional office which is protected by a palisade fence. The application of territorial reinforcement in the three regional offices of the Mangaung Metropolitan

Municipality is implemented through the fences around the premises, lights to increase visibility at night and sidewalks (Coppernica, 2020:402).

3.12.1.2 Gates

The use of security gates has proven to be an effective measure to reduce theft and burglaries in facilities (Rhodes, 2020: n.p.). Gates are significant to facilitate and control access for employees, customers, and visitors to the facility. Therefore, gates need to be controlled to ensure that only authorised people and vehicles pass through them (Fennelly, 2013: 342). They are a common method to restrict vehicle and pedestrian access to premises and properties and some argue that for a gate to be effective, it needs to be integrated with other security measures (Rhodes, 2020: n.p.). Gates are installed at entry and exit points on a fence to provide perimeter security around the premises to help control access to certain sites by restricting the movement of people and vehicles (Baker, 2017:38).

ISIS International (2009) maintains that gates are effective in preventing unauthorised access to a facility when integrated with closed-circuit television (CCTV) (ISIS International, 2009:12).

Therefore, security gates are an effective access control measure if they are operated to regulate one entrance into and out of the premises. The benefit of this is that limiting the number of access entry points is an effective way to prevent criminal activities because the more the facility has, the more criminals have easy escape routes. Any other alternative entrance and exit other than through the gates will raise suspicion which will result in detection and ultimately, apprehension (Atlas, 2013:70). The three regional offices of the Mangaung Metropolitan Municipality in Bloemfontein use ordinary gates that are not integrated with an alarm system or closed-circuit television (CCTV). These gates remain opened during the day to allow members of the public free entrance and exit except when the cash-in-transit company is collecting the municipal revenue from rates and taxes or at night (Swart, 2020: n.p.).

3.12.1.3 Turnstiles

Turnstiles are security barriers used to restrict and manage human traffic flow at access control points (Homeland Security, 2015:13). Turnstiles can be used as the main method of access control in a lobby or in combination with the access control of other exits and entrances by permitting exit without the use of the access control system but entering only through an access control entrance (British Security Industry Association, 2016:35). Baker (2016) maintains that turnstiles are regarded as a supplementary access control measure to assist both the guards and receptionists while controlling access into a protected area (Baker, 2016:106). According to ASIS International (2009), turnstiles are effective to control the density of movement of people and as well as to minimise 'piggybacking', which is an unlawful act of gaining unauthorised access into a facility by following a person with legitimate permission in and out of buildings. Turnstiles operate like a revolving door to allow only one person at a time access into the premises and building (ASIS International, 2009:12).

Turnstiles are valuable in preventing tailgating which is a situation where an authorised person facilitates the entrance of an unauthorised and unverified person (Homeland Security, 2015:13) A recent study conducted by Ritchey (2019) on enterprise security executives, regarding perceptions about the risk of tailgating, found that the majority of respondents (77%) believed that guards and other physical barriers like turnstiles were the most effective way to prevent tailgating (Ritchley, 2019:52).

ASIS International found that turnstiles are effective when coupled to a biometric access control system for thumbprints and the data connected to the control room. People’s details, including their photos, are taken, and loaded on the system with a specific number assigned to each person, which will work in conjunction with their thumbprint (ASIS International, 2009:14). This is only used at the Bram Fischer building which is the head office of Mangaung Metropolitan Municipality.

The British Security Industry Association (2016:35) suggests that the following types of turnstiles are distinguishable in restricting the entrance of people to buildings: (a) turnstiles that are integrated with an alarm system that will trigger in the event of unauthorised entry into a facility, (b) mechanically operated sliding and revolving doors or gates that open an entrance and close when it is completed, (c) rotating entrance gates to allow wheelchairs and wide deliveries, (d) security booths that have two doors to allow a person entrance at the first door then close before the second door opens, (e) a revolving security door that is integrated with an access control system (British Security Industry Association, 2016:35).

The above types of turnstiles, according to the British Security Industry Association (2016), consist of the following security features to enhance their effectiveness in managing access control: (a) anti-pass back to prevent the utilisation of the access device of another person who has already gained access into a facility (British Security Industry Association, 2016:35), (b) anti-tailgate with an alarm device to prevent an unauthorised person from entering or exiting an area by pushing him- or herself in behind an authorised person, (c) multi-card usage flexible enough to accommodate different tokens to grant access when registered users have different devices assigned to them, (d) lift control device to grant access to different floors in the building and (e) automatic number plate recognition (ANPR) which uses a camera to capture the image of the vehicle number plate to grant them access into and out of the parking are relying on stored information in a database (British Security Industry Association, 2016:40).

3.12.1.4 Mantraps

These are designed to trap an individual by locking them in a small room until their identity is verified. It is designed to deliberately delay the entry of an unauthorised person until the security official responds to acts of security breaches (Niles, 2011:10). Mantrap doors allow one person at a time to enter and prevent unauthorised persons entering by following a person who has been granted legitimate access into the facility (Niles, 2011:10).

3.12.1.5 Closed-circuit television (CCTV)

Closed-circuit television is used in areas 24/7 from a central location to monitor the perimeter, including areas that might be obscured from guards (Rao, 2016:66).

According to Fennelly (2012:262), CCTV cameras are also installed at access control points to monitor and record access into, within and out of the facility. Rao (2016) maintains that although CCTVs are effective in monitoring movements, they are passive devices that can only monitor intrusions but cannot prevent them and must be integrated with other security measures to be effective (Rao, 2016:66). A study conducted in 2019 on the use of CCTV surveillance systems for crime control and prevention in Johannesburg and Tshwane found that CCTV was effective in combating crime when integrated with other security measures, unlike when it is applied alone (Moyo,2019: IV).

3.12.1.6 Locks

Locks are an essential component of physical security to prevent unauthorised physical access into a facility (Hutter, 2016:433). They are most widely used as a physical access control measure to prevent intruders from unlawfully gaining access into premises and buildings. The disadvantage of locks is that they can be used by anybody, without a track record that can be monitored concerning their previous use (McCrie, 2007:296). According to Truett (2015), locks are useful to secure and restrict access to things that need protection. He identifies several categories of locks such as key-in-knob which is a key cylinder set into a knob or level handle to open a door, mortise which is used for commercial purposes to operate the locking and unlocking of doors, padlocks that are used by government departments to protect classified material and weapons (Truett, 2015:95). Locks are also regarded as a preventative physical access control measure in doors and windows to prevent unauthorised people from gaining access to a secure area (Dingle, 2015:95).

The following are different types of locks that are used as physical security barriers to manage access control within premises and buildings.

(a) Mechanical locks

Mechanical locks are said to be the oldest forms of access control (Moses, 2016:669). These locks include door locks, cabinet locks and padlocks to prevent access by unauthorised people. However, these locks are vulnerable to attacks such as picking in which a person can use three-dimensional printing (3D) to manufacture a specialised tool to manipulate the functioning of these locks or by making an imprint that uses a blank key to develop an impression of the target lock. Finally, by copying and duplicating a key for use to gain access into a facility or building (Moses, 2016:670).

(b) Electrified locks

Electrified locks are operated digitally and are opened when a code is entered and open when a signal is received after the identification and authentication of the user to gain access to a property (Fay, 2018:172). Electrical locks allow doors to be opened and closed by a remote control, sometimes using push buttons, motion sensors, card readers, digital keypads or a biometric device (Moses, 2016:670).

(c) Electromagnetic locks

Electronic magnetic locks are an electronically controlled means of allowing entry through a door (Graichen, 2012: n.p.). They are commonly used in a delayed exit system of a building. The purpose is to allow people to exit a building in the event of an emergency and simultaneously provide a security measure against unauthorised entry and exit. The door is activated by pressing down the panic bar which will then trigger an alarm, opening the door for approximately one to three seconds. These locks consist of an electromagnet which is attached to the door frame, coordinated with safety codes attached to doors that are important to the building's design (Graichen, 2012: n.p.).

(d) Credential operated locks

According to Caputo (2014), credentials are something an individual has, something he knows and something unique about an individual (Caputo, 2014: n.p.). Credential operated locks rely on a unique device swiped to a card reader where access is controlled by checking the identification of the cardholder and comparing it with information stored in the database and thereby permit or deny entry. They also provide a track record and register the time of access into a facility (Moses, 2016:670).

(e) Combination locks

Combination locks operate mechanically and electronically, using a keypad to select numbers or letters that are stored, to release the locking mechanism. This relies on the card reader as well as the biometric features (Moses, 2016:670). Fay (2018) maintains that combination locks are incorporated in padlocks, safes, vaults and doors and use tumblers inside them that range from three, four or five used in high-security areas to release the locking mechanism (Fay, 2018:173).

3.12.1.7 X-ray machines

According to the United States Nuclear Regulatory Commission (USNRC) (2011), x-ray machines are used to assist access control to determine that unauthorised items and packages are not brought onto premises. They are usually employed at airports (United States Nuclear Regulatory Commission, 2011:2.29). This security measure consists of X-ray machines and metal detectors used to detect and identify dangerous objects that might endanger the lives of people within the premises. These devices, together with security officers and sniffer dogs, are used to detect contraband being brought onto premises (ASIS International, 2009:20).

3.12.1.8 Vehicle Access Control

Access to premises is controlled by using measures such as cardboard placards, stickers, radio frequency identification (RFID), tags, bar codes, special licence plate and electronic tags (ASIS International, 2009:20). This can also be done manually by being operated by a security officer or electronically through proximity cards to regulate access into a facility (ASIS International, 2009:20).

3.12.1.9 Administrative access control measures

Administrative access control measures are structured processes that employees, contractors and visitors must follow when entering and leaving secure areas. Like other components of security, administrative arrangements provide clear guidelines and processes for activities to organisations to implement access control (Hour, 2012: n.p.). The administrative access control measures are important to prevent and detect inappropriate access practices at facilities through various policies and procedures that define the different roles and responsibilities of users (Rao, 2016:66). Therefore, access control administrative measures are important to assist security personnel with recording-keeping of all activities related to access control and of liaison between security management and the clients of an organisation (Norman, 2016:250).

3.12.2 Policies and Procedures that regulate access control at Mangaung Metropolitan Municipality

Policies and procedures are critical elements of successful access control programmes. The following is a demonstration of how policies can provide an effective access control management system within organisations: They define the roles and responsibilities of all stakeholders within the premises such as employees, contractors and visitors (Rao, 2016:66). ASIS International (2009:21) holds the view that access control policies and procedures are a mandatory security requirement for access control management, vehicle access control measures, removal of property from the facility, wearing of badges, sharing of personnel identification numbers or pins, sharing of access cards, tailgating or piggybacking, searching of packages and bags, list of prohibited materials, access hours and levels of access, credential tampering and replacement, accommodation of disabled or physically impaired people, use of explosives detection and preventive maintenance of equipment (ASIS International, 2009:21).

The following policies and procedures apply to the Mangaung Metropolitan Municipality for the implementation at an access control point: (a) All visitors must complete the visitor's register which is countersigned by the security officer, (b) a copy of an ID document or driver's licence must be produced for every visit to verify the identity of the visitors, (c) dangerous objects and other contraband are not allowed into the premises, (d) all vehicles will be searched when leaving the premises of the Mangaung Metropolitan Municipality and (e) employees visiting the buildings after hours have to complete an attendance register.

3.12.2.1 Personnel Access Control

Apart from these technological applications, there is the human element which is made up of high-quality security personnel at access control points, providing the backing and support necessary for effective access control (Mahambane, 2014:10). This is because they are on the ground and they can provide adequate surveillance and prompt response to mitigate threats that can harm the organisation.

To enable access control to be effective, security officers deployed at access control points need to perform the following functions: screening employees and visitors in the reception area, controlling access to the facility at other points, escorting visitors, inspecting packages and vehicles, issuing visitors with badges for use during the duration of the visit and collected before departure out of the premises, preventing tailgating and monitoring the movement of employees and visitors at secure areas (Mahambane, 2014:10). The Mangaung Metropolitan Municipality access control policy requires security offices to apply the above functions to regulate and control the movement of people into buildings by ensuring that only those who are authorised are permitted and those without the necessary authorisation are denied entry.

3.12.2.2 Badges and ID Cards

At the Mangaung Metropolitan Municipality, employees are not issued with badges and cards for identification purposes. According to Homeland Security (2015:16), badges bear the holder’s photo and personal details together with the name and logo of an organisation. They are useful in providing evidence that the bearers are authorised to be on the premises and buildings of an organisation as well as to prove their identities. These come in the form of smart cards, name tags and identification cards that are integrated with access control systems, to allow for the validation of individuals (Truett, 2015:99).

Hutter (2016:259) identifies the following four most common access control identity cards: (a) personal recognition system. This is regarded as the simplest of all in which entry is granted based on individual recognition, established reason to access the facility and lastly, the person on the access roster, (b) single card/badge system in which permission for access is based on specific numbers, colours and letters indicated on the card, (c) card/badge exchange system in which two cards or badges contain the identical photo of the individual where one card is issued upon entrance and exchanged with a second one while the bearer is in the facility; when the individual leaves the facility, the second one is returned to him/her and (d) multiple cards/badges that necessitates an exchange of cards at the entrance of each security area and are gives only to individuals with access rights to a specific area (Hutter, 2016:259).

3.12.2.3 Electronic access control measures

Electronic access control measures consist of electronic elements together with physical elements to facilitate access for authorised people to the premises. This access control measure uses computer-based technology to monitor access through devices that are programmed and swiped to card readers which are efficient and flexible to secure the buildings (Fennelly,2016:11). According to Norman (2012:3), electronic access control measures entail electronic systems that authorised people to a controlled space through the presentation of access credentials such as magnetic cards and smart cards to a reader (Norman,2012:3). As a precautionary measure to prevent the spread of Covid 19, the Mangaung Metropolitan Municipality replaced the finger biometric scanning devices with proximity cards at the entrances and the basement parking. Rao (2016:64) maintains that access control is a system that can grant or deny access of an individual into and out of the facility through the following systems:

3.12.2.4 Knowledge-based access control technique

Knowledge-based access control technique entails something a person knows which usually revolves around the fact that there is some sort of knowledge that only the organisation that operates the access control knows and which is stored and coded in the brains of people to prove their identity. Examples of this device are passwords, pins and codes (Esfandi & Sabbari, 2014:152). At the Bloemfontein regional office, access for employees is implemented through a keypad device that uses a pin code allocated to each employee.

3.12.3 Token-based access control technique

The token-based access control technique entails an authentication process based on devices being in the possession of people and are programmed into an access control system to prove the identity of a person for admission into a facility (Esfandi & Sabbari, 2014:152). This is made up of three devices that are mechanically operated using a set of keys that perform different functions, both electric and mechanical, that use a push button to operate a set of relays and lastly, a computerised keypad programmed to open the door (Bowers, 1988:67).

In elaborating more on these devices, Norman (2012) identified the following security measures for use in this type of identity verification to enhance access control.

3.12.3.1 Magnetic stripe cards

This is the most common type of access card, consisting of a magnetic strip that when swiped into a machine, gives access to a facility. These cards originate from ATM cards and their latest application is proximity cards which are used by registered users to open booms at the entrances of parking areas and universities (Norman, 2012:51).

3.12.3.2 Bar-coded cards

This card contains a bar code that is read when the card is swiped in a reader. Niles (2011:8) asserts that the bar-coded card is used as a minimum-security measure, especially when there are many readers as well as high traffic volume of entrance at a given access point.

3.12.3.3 Proximity cards

Proximity card access control systems are said to be the most suitable way to control access to a building or facility (Moses, 2016:671). This argument is taken further by maintaining that there are two types of proximity cards: a passive card which is normally kept in a wallet or purse and held close to a reader to activate access and also an active proximity card with a range of two metres in which a card can be read from inside a vehicle (Moses, 2016:671).

Hutter (2016:1) maintains that the proximity cards are scanned into the readers via the radio frequency identification (RFID) to determine whether the user has authorised access to enter the facility. When the card is presented to a system, it provides a history of recorded events stored in the database which can be easily retrieved by making use of the cardholder's credentials such as identity, the duration of access and any other information that the organisation can use to keep track of the user (Umbrella Technologies, 2019:5).

The use of proximity readers in physical access control contains passive tags powered by an electronic magnetic field to unlock the doors once the signal is received and verified. These readers can track the movements of an item that is connected to the network to trigger the alarm system if it is unlawfully removed (Hutter, 2016:2).

Although these cards are effective to withstand 3D printing, they are vulnerable to attacks from a 'man in the middle', which is a situation where an attacker acts as a middleman to intercept a transaction and pass it on. Secondly, a relay attack is a situation where an attacker relays communication between the reader and the card (Moses, 2016:671).

3.12.3.4 Smart cards

This card, like the proximity card, contains a built-in silicon chip for embedded on board data storage. They have coded memories and microprocessors with the technology in them providing many possibilities, particularly with proximity card-based access control systems. These cards are divided into two types: a contact card that has a contact point in front to transfer data when it is inserted into a device and a contactless card that uses antennae to communicate with the card reader through the magnetic signal (Hutter, 2016:2).

3.12.3.5 Keypads

Keypads are a common and reliable method of access control that consists of unique codes known as personal access code (PAC) or personal identification number (PIN). ID readers contain several digits known to the authorised user to gain access into the perimeter or building (Niles, 2011:8). Norman (2012:52) argues that they are relatively cheap and easy to use but vulnerable to duplication in the event an authorised person gets to know the code.

Therefore, access control only permits entry to authorised employees and contractors should have access cards to enter the building. These cards enable employees and contractors to move freely within the building by logging all their accesses to include date, time, specific floor, and card identification numbers.

3.13 BIOMETRIC ACCESS CONTROL TECHNIQUE

Biometric access control is a system that helps to prevent unauthorised individuals from accessing facilities and include physical access control measures and logical access control based on biometric authentication (Thales,2020:n.p.). The application of biometrics to recognise people is derived from images of fingerprints, hand vein patterns, retinas, irises, facial expressions, signatures, voice patterns and body temperature to authorise their access to premises (Norman, 2017: n.p.).

Sabhanayagam (2018) explains that biometric is a Greek word *bios* meaning life and metric or *metrikos* meaning measure which is directly translated into "life measurement". He argues that biometrics is an ancient technology that was used by the Egyptians to identify and authenticate people through facial recognition by distinguishing between known and unknown people (Sabhanayagan, 2018:2276). Boukhonine (2005:937) mentions an Egyptian administrator who started using unique physical characteristics to identify contract workers to ensure the equitable distribution of food rations.

Other developments in the application of biometrics involve the New York State prison using fingerprints to identify criminals in 1903. The FBI started with the analysis of fingerprints in 1921 (Kelsey, 2019:665). Another application of this technology was the building of a world database of terrorists by the FBI by collecting the fingerprints and scanning the irises and facial images of Iraqis and Afghans to facilitate identification and authenticating their identities (Kelsey, 2019:665).

With the rise in the application of computers in the 1990s as well as the Al-Qaeda attacks on the USA on September 11 in 2001, the US government and private sectors started to use biometrics to identify and authenticate individual access to both tangible assets such as buildings and premises as well as intangible assets such as computer networks (Munanga & Illaiah, 2014:53).

Kelsey (2019:665) maintains that biometric techniques is synonymous with the way that human beings identify one another. It uses an automated system to identify and authenticate human beings by measuring their unique physical characteristics like fingerprints, retinas, irises, hand geometry, hand vein patterns, ear shapes and facial recognition systems, and biological traits such as voice recognition, keystroke, signature and gait analysis through comparison to traits and characteristics stored in a database (Kelsey, 2019: 665).

This explanation is taken further by Ashbourn (2014) who maintains that biometric technology is a scientific recognition of people based on the features of their bodies, using a computerised system to verify their identities (Ashbourn, 2014:14). This technology is widely used by government and private organisations worldwide, to maintain both physical and logical access control to buildings and premises as well as highly secure areas like servers and computer systems points. The purpose is to prevent both identity fraud and security breaches in these areas (Harris, 2013:259).

Biometric identification and authentication have emerged as the most reliable form of recognition that is difficult to forge or manipulate. Security codes, passwords, hardware keys, smart cards, magnetic stripe cards, ID cards and physical keys can be lost, stolen or duplicated and passwords can be forgotten, shared or observed (Harris, 2013:259). At the Mangaung Metropolitan Municipality, the biometric system is applied through a fingerprint scanning device that is mounted on the turnstiles at the entrance of the Bram Fischer building and the underground parking to operate the boom gate.

3.14 BASIC FUNCTIONS OF BIOMETRICS

Thales (2020: n.p.) maintains that the biometric application has been historically used for military access control, civil and criminal identification and later by sectors such as banking, retail and mobile commerce (Thales, 2020: n.p.).

The use of biometric technology is applied in the following situations to ensure the protection and validation of individual identities (Gennouni, Mansour & Ahaitouf, 2019:5):

By law enforcement agencies and the justice system to identify and recognise individuals alleged to have committed acts of crime; at ports of entry to identify travellers, migrants and passengers entering the country; lastly, for both private and public use as well as personal computer (PC) network access, physical access control, automated teller machine (ATM) and surveillance (Gennouni, Mansour & Ahaitouf, 2019:5).

Gennouni, Mansour and Ahaitouf (2019) identify the following modes to enhance the recognition of human characteristics and behaviour through a biometric system:

Enrolment mode, whose aim is to collect information about who to identify from information captured on the database which is then represented in a digital form. Verification mode which proves the identity of a person by comparison with the biometric information stored in the system and database through a personal identification number, username or smart card. Lastly, identification mode recognises an individual by matching his credentials with information on the database (Gennouni, Mansour & Ahaitouf, 2019).

Apart from the above uses, biometrics are used by both the government and private sectors for access control installed and are connected to doors and entrances to validate the credentials of users through information captured in the database (Rao, 2014:9).

3.15 OVERVIEW OF THE IMPLEMENTATION OF ACCESS CONTROL IN THE MANGAUNG METROPOLITAN MUNICIPALITY AND THE THREE REGIONAL OFFICES

Over the years, the Mangaung Metropolitan Municipality has sustained numerous losses attributed to security breaches which had both financial and reputational consequences due to inadequate and ineffective physical access control measures, with losses estimated to be R350 million over the last five years (Weekly, 2015:1). Common security breaches were unauthorised access to buildings and premises, theft, armed robbery, vandalism, damage to property and threats to the safety of employees, political leadership, community members, contractors and suppliers (Mangaung Metropolitan Municipality risk register, 2017/18).

These incidences required the Mangaung Metropolitan Municipality to implement access control in accordance with two important legislations such as the Trespass Act No 6 of 1959 whose purpose is to prohibit unlawful entry or presence on lands and buildings by giving the owner, in this instance, the Mangaung Metropolitan Municipality council, the authority to deny or evict such persons under certain circumstances. In other words, this act prohibits people who are not authorised to enter the premises of the municipality without permission being granted to them through reservations of their granted entry (Trespass Act 6: 1959, Section 1).

The application of this act empowers the City Manager to remove any person from the premises if there is a reason to believe that permission was not granted for him/her to be on the premises.

The second piece of legislation is the Control of Access to Public Premises and Vehicles Act 53 of 1985 as amended, which requires the City Manager to implement access control measures in the Mangaung Metropolitan Municipality premises and buildings by monitoring the movement of people, vehicles, and materials into, within and out of the premises (Control of Access to Public Premises and Vehicle Act 53: 1985, Section 2). In terms of Subsections 2.2 of the act, heads of departments and institutions which, in the case of the Mangaung Metropolitan Municipality, is the City Manager who is the head of administration, is required to implement access control measures to ensure that any person gaining access into the premises of the municipality is safe, has a valid reason to enter and is authorised and that the department employees will not be exposed to any danger or any form of security breaches (Control of Access to Public Premises and Vehicle Act 53: 1985, Section 2).

The Mangaung Metropolitan Municipality needs to institute measures to control access and movement in their premises with specific reference to its three regional offices, to control the movement of employees, visitors, and contractors through proper verification of their details (Mangaung Metropolitan Municipality security policy, 2011:44). Subsection 2.2 (g) of the Control of Access to Public Premises and Vehicle Act 53 of 1985, Section 2, furthermore entitles the City Manager to authorise searches of everyone entering and exiting the premises. In addition, the Act also allows for the recovery of any property of the municipality which might have been unlawfully removed as well as to confiscate any object that might endanger the lives of occupants of the building, visitors, contractors, and stakeholders. Therefore, all vehicles, both private and belonging to the Mangaung Metropolitan Municipality, must be searched when entering and leaving the premises to ensure that there is no unauthorised removal of assets and property (Control of Access to Public Premises and Vehicle Act 53: 1985).

In light of these provisions, the Mangaung Metropolitan Municipality is required to implement integrated access control measures at its premises and offices and to safeguard its personnel, clients, stakeholders, properties, business continuity and processes. The following access control measures are implemented within the Mangaung Metropolitan Municipality's premises:

In Bloemfontein, the Bram Fischer building houses the head office of the municipality. At the entrance point, a fingerprint biometric system is mounted on turnstiles to grant access to both employees and councillors to enter the building and to gain access into the basement parking. This system is monitored by the surveillance system which is integrated into the close circuit television (CCTV) and an alarm system. At the entrance point to the main building, contract security guards are deployed to manage access for visitors into the main building. To manage access at the offices of the Executive Mayor, the Speaker, Chief Whip, Members of the Executive committee (MMC's), the City Manager and heads of departments in the Bram Fischer building, the Mangaung Metropolitan Municipality uses keypads that are operated by using passwords together with VIP protection services.

In the three regional offices which are the focus of the study, the following access control measures are in place:

The Bloemfontein regional office which is situated adjacent to the Department of Home Affairs regional office has two gates, the first is used by both organisations for vehicular entrance. The second gate is used for both the pedestrian entrance into the premises and exit for the vehicles. These gates remain open during the day and are only closed at night and during the cash pickup by the cash-in-transit vehicles. Access control into and out of the premises as well as at the rates hall and underground parking is not regulated because the security guards are only positioned at the entrance of the administrative building to regulate the entrance of visitors.

The Botshabelo regional office situated next to the magistrate court has two gates. The first one is used for the entrance of vehicles and is manned by security guards whereas the second one is used by pedestrians and has no security guards. These gates remain open during the day and are only closed at night and during the cash pickup by the cash-in-transit vehicles. There are no security guards to operate access control into the main building, rate hall and the old council chamber.

Lastly, the Thaba Nchu regional office is situated next to the public library. It has one gate which is used by both vehicles and members of the public, including the employees to go in and out of the premises. There are no guards at the gate, only at the main entrance of the administrative building to operate access control. The same applies to the other two regional offices, the gate remains open during the day and it is only closed at night and during the cash pickup by the cash-in-transit vehicles. In all these three regional offices there is no proper identification of both employees and members of the public entering the buildings and premises as none is issued with ID cards and badges. Although the premises are protected by the palisade perimeter fences, these have not been integrated with surveillance and detection measures such as the closed-circuit television and alarm systems.

3.16 THEORETICAL FRAMEWORK

In this study, the researcher is guided by different approaches and theories relevant to access control as a crime prevention measure in the Mangaung Metropolitan Municipality regional offices.

3.16.1 Routine Activity Theory

In contrast to most criminological theories that focus on the offenders' motivation in committing a crime, the routine activity theory emphasises explaining circumstances that are required for a crime to be committed (Smith, 2013:106). According to the routine activity theory, crime is believed to be a result of everyday behaviour which occurs more frequently where people's daily activities create the most opportunities for a motivated offender in the most profitable crime and with the least chance of retaliation. This clearly explains the number of crimes occurring at the Mangaung metropolitan regional offices that, through the surveillance tactics of the criminals, presents motivation and opportunity as a result of the perceived deficiencies of the security measures currently in place.

The occurrence of crime is viewed as an event that occurs at a specific location and time as a result of a merging of the following elements: (1) a motivated offender who is prepared to commit the offence; (2) a suitable target, such as a victim to be assaulted, a piece of property to be vandalised or assets to be stolen and (3) the absence of a capable authority figure to prevent crimes from occurring (Clarke, Cohen & Felson, 1979:588). When these three elements are present at the same time and place, crime will take place (Cohen & Felson, 1979:590).

The routine activity theory recommends the presence of a capable guardian which in this context, is effective access control to prevent the occurrence of crime through implementing security measures such as physical barriers like fences, locks, walls and gates; electronic barriers like closed-circuit television (CCTV) and procedural barriers such as identification badges and mobile guards to impede the ingress of an offender into a facility (Cohen & Felson, 1979:590). This function at the Mangaung Metropolitan Municipality is performed by contract security guards under the oversight of law enforcement officers and the regional general managers.

The routine activity theory further suggests that the organisation of routine activities in society create opportunities for crime. In other words, the daily routine activities of people, be it at work or the route they travel, strongly influence when, where and to whom crime occurs. The weak access control measures at the regional offices motivate and influence criminals who see this as an opportunity to breach the current security arrangements.

3.17 CONCLUSION

This chapter presented a discussion on the implementation of access control through a review of literature from various sources such as books, articles, journals and internet resources. Aspects covered include the evolution of access control as a security measure to restrict and regulate the movement of people in and out of the premises to protect assets, lives and property.

The two types of access control, namely physical and logical access control measures were discussed with more emphasis placed on physical access control measures which constitute the epicentre of the study.

The review of the literature found that the application of an integrated approach of access control, using the above different types of security measures, creates a management system that will help the organisation to maintain a safe environment for both employees and visitors as well as reduce losses that can be caused by various forms of security breaches. Ideally, access to the facilities of any organisation should be restricted only to those people who have a valid business purpose. This also applies to an organisation as large as Mangaung Metropolitan

Municipality combined with its regional offices, where employees do not know each other. The implementation of access control should be based on the allocated authority to restrict access to persons and vehicles through the implementation of security control measures like gates, doors, turnstiles, keypads, card readers, personnel, policies and procedures which are integrated with CCTV and intrusion alarms.

In view of the above, it is evident that the importance of access control cannot be overemphasised. Access control is an important element of security that provides physical security for small and large organisations. Access control systems secure areas such as buildings and facilities through restricting and allowing authorised people entry into the premises and denying those likely to cause harm to property, people and resources of the organisation.

The next chapter presents the data analysis and research findings of the study.

CHAPTER 4
DATA ANALYSIS AND INTERPRETATION OF FINDINGS

4.1 INTRODUCTION

This chapter deals with the interpretation and analysis of the findings from the data collected from the research participants. Data was collected by conducting one-on-one unstructured interviews with participants using a semi unstructured interview schedule. In this study, the analysis interpretation of the collected data involved the process of trying to make sense of the information collected and draw the conclusions, significance, and implications of the findings. In Chapter One, the aims and objectives of the study were presented, and these are briefly repeated below to provide contextual relevance for the analysis and interpretation of data. The objectives of the study are to examine the effectiveness of the existing access control measures currently in place within the three regional offices of the Mangaung Metropolitan Municipality, evaluate the security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality's regional offices at access control points and to make recommendations on the types of access control measures to be used to mitigate the impact of the risk factors.

To achieve these objectives, data for the study was collected from forty-five research participants employed at the three regional offices of the Mangaung Metropolitan Municipality. The researcher recorded interviews using a tape recorder and a notebook which was transcribed daily while still fresh in the researcher's memory. Furthermore, the interview transcripts were analysed and the responses by the participants were documented and grouped together to pick up common themes and categories for purposes of analysis (Creswell, 2016:175).

The interview schedule used to collect data comprised four sections: Section A consisted of the demographic information of the participants; Section B covered an overview of the various aspects of access control at Mangaung Metropolitan Municipality regional offices; Section C dealt with the security risks and vulnerabilities confronting the Mangaung Metropolitan Municipality regional offices at access control points and lastly; Section D contained the recommended access control measures that needed to be implemented at the three regional offices.

4.2 SECTION A: DEMOGRAPHIC INFORMATION

The demographic profile is important for the study because it determined the relevance of the participants for inclusion in the research.

4.2.1 Demographic information of research participants

The research participants were distributed across three regional offices at the Mangaung Metropolitan Municipality (See Table 4.2.1). To differentiate the participants from the three regional offices and for ease of reference, the following acronyms were developed: **[BL]** for the Bloemfontein regional office **(BL –research participants= 1-20); [TN]** for **Thaba Nchu** regional office **(TN research participants= 1-10) and** lastly**, [BT] for Botshabelo** regional office **(BT research participants= 1-15)**

The following demographic profile of the research participants is presented in Table 4.2.1

Table 4.2.1: Demographic Information of Participants

Research Participants	Gender	Age (Years)	Race	Marital status	Highest qualification	Length of years of service	Region where Employed
BL 1	Male	52	Black	Single	Post graduate	15	Bloemfontein
BL 2	Male	47	Black	Single	Matric plus courses	17	Bloemfontein
BL 3	Male	44	Black	Single	N2	15	Bloemfontein
BL 4	Female	26	Black	Single	B degree	5	Bloemfontein
BL 5	Female	32	Black	Married	Matric	5	Bloemfontein
BL 6	Female	46	Black	Single	Grd12	15	Bloemfontein
BL 7	Male	32	coloured	Married	Matric	13	Bloemfontein
BL 8	Male	56	W	Married	NTS 5	14	Bloemfontein
BL 9	Male	48	Black	Married	Matric	22	Bloemfontein
BL 10	Male	29	Black	Single	Matric	10	Bloemfontein
BL 11	Female	32	Black	Married	Matric	7	Bloemfontein
BL 12	Male	29	Black	Single	B degree	6	Bloemfontein

BL 13	Female	49	Black	Single	Grd 12	5	Bloemfontein
BL 14	Female	33	Black	Single	Diploma	7	Bloemfontein
BL 15	Female	41	Black	Single	Grd 12 Psira E,D,,C	1	Bloemfontein
BL 16	Male	39	Black	Married	BTech Civil Engineering	13	Bloemfontein
BL 17	Male	50	Coloured	Married	B.Com	29	Bloemfontein
BL 18	Male	28	Black	Married	Post-graduate	9	Bloemfontein
BL 19	Female	63	Black	Single	BTech Environmental Health	17	Bloemfontein
BL 20	Female	49	Black	Married	GRD 11	22	Bloemfontein
TN1	Male	47	Black	Married	Grd 11	22	Thaba Nchu
TN2	Male	33	Black	Married	Matric plus Psira grades E,D,C	2	Thaba Nchu
TN3	Male	51	Black	Married	Masters	28	Thaba Nchu
TN4	Female	64	White	Married	Matric	41	Thaba Nchu
TN5	Female	56	Black	Married	Matric plus NQF 7	37	Thaba Nchu
TN6	Male	50	Black	single	Grd10	27	Thaba Nchu
TN7	Female	49	Black	Married	Grd 12 plus Diploma in management	21	Thaba Nchu
TN8	Male	35	Black	Single	Btech	5	Thaba Nchu
TN9	Male	29	Black	Single	Matric	5	Thaba Nchu
TN10	Female	39	Black	Married	Traffic Diploma	10	Thaba Nchu
BT 1	Male	50	Black	Married	Matric	25	Botshabelo
BT 2	Male	53	Black	Married	LLB	27	Botshabelo
BT 3	Female	51	Black	Single	Matric	22	Botshabelo
BT 4	Male	46	Black	Married	B degree	20	Botshabelo
BT 5	Male	48	Black	Married	Grd 11, PSIRA E,D,C	4	Botshabelo
BT 6	Female	35	Black	Married	Matric Psira Grd E,D,C	1YR six months	Botshabelo
BT 7	Male	46	Black	Married	Diploma	14	Botshabelo
BT 8	Male	49	Black	Single	Diploma	12	Botshabelo
BT 9	Female	26	Black	Single	B degree	5	Botshabelo
BT 10	Male	51	Black	Married	B degree	15	Botshabelo
BT 11	Male	49	Black	Married	Matric	22	Botshabelo
BT 12	Female	38	Black	Single	Diploma	16	Botshabelo
BT 13	Female	32	Black	Married	Matric	18	Botshabelo
BT 14	Female	47	Black	Married	Matric	27	Botshabelo
BT 15	Male	56	Black	Married	PhD	17	Botshabelo

4.2.2 Data analysis and discussion of findings

4.2.2.1 Gender of the research participants

In this study, the number of male participants employed at Mangaung metropolitan regional offices is greater than females. Males constituted 60% and 40% females. The reason for this can be attributed to the fact that these are service delivery points in which the majority of employees performing those functions are males. The majority of that females are in the Bram Fischer building where more administrative functions are performed.

Age of the research participants: The ages of all races of the research participants varied in all the regional offices. Black males between 28–35 constituted 17%, 35–45 made up 8% and 45–65 made up 35%. Females between 28–35 constituted 15%, 35–45 made up 22% and 45–65 made 20%.

Race of the research participants: In this study, blacks constituted the highest percentage at 90% and the reason for this is that two of the regional offices, Thaba Nchu and Botshabelo were the former homelands of Bophuthatswana and Qwaqwa.

Marital status: In the study, 24 employees were married which constitutes 53.3% of the target population, whereas 21 employees were single and constitutes 46.6%.

Highest qualifications: Fifteen (15) participants in the study had matric certificates (33 %); three (3) participants had TVET qualifications (6%); four (4) had diplomas (8%); six (6) had bachelor's degrees (13%); five (5) participants had post-graduate qualifications (11%) and four (4) had Grades 10 or 11 (8%). Employees with matric made up the largest number of participants partaking in the study.

Length of years of service: In summary, the majority of the participants in the study were males, black, have matriculated, are married and had 20 to 30 years of service.

4.3 SECTION B: ASPECTS PERTAINING TO ACCESS CONTROL AT MANGAUNG METROPOLITAN MUNICIPALITY

This section responds to the first research objective of the study which is to evaluate the current access control system in place within the Mangaung Metropolitan Municipality regional offices

4.3.1 Analysis and discussion of findings

The researcher analysed the data from the participants using Creswell‘s six steps of qualitative data analysis (Creswell, 2016:175). The first step necessitated the organisation and preparation of data for analysis. This was done through transcribing and recording the responses of the participants to questions that were posed using the interview schedule. Secondly, the researcher read and looked at the data to see the tone, general ideas and credibility of the information furnished by the research participants. The third process involved the coding of the data collected. This was done by placing data into segments and giving it a label to reflect its meaning (Creswell, 2016:175).

In the fourth step, the researcher generated themes by looking for the most common responses from the questions contained in the interview schedule. In this way, the researcher identified several themes and categories from the data collected.

The fifth step entails the researcher using a narrative passage to determine areas of commonalities in the responses of the participants during the interviews. Lastly, the data was interpreted with findings and conclusions made (Creswell, 2016:175).

To achieve the objectives of the study as mentioned in Chapter One, the following questions were posed to the research participants.

Research Question 1: ***What existing access control measures are in place in your regional office and how effective are these measures to protect property, assets, employees, contractors and members of the public?***

4.3.1.1 Theme 1: Awareness of access control measures

According to **participants BL1–20,** access control measures in place in this regional office consist of private security guards deployed at the entrance of the main building which houses employees from different directorates, members of the municipality public account committee (MPAC) and at the rates hall where cashiers are placed to collect payments of rates and taxes. They also mentioned the perimeter fence and gates on the western side, adjacent to the houses, one at the back and the other one in front to facilitate entrance from the Home Affairs regional office.

Participant BL1 added that the keypads are no longer operational for employees to access the main building, **BL 4**–**14** mentioned the boom gate at the entrance of the basement parking, participant **BL 16** mentioned that there is a roller door at the rates hall to complement a deployed security guard for control access control of visitors coming for the payment of rates and taxes.

Participants BL 3–**20** mentioned the doors as one of the access control measures into the buildings to restrict access at night and after hours. Lastly, **BL 13** maintained that there are closed-circuit television (CCTV) cameras that are not functional which results in daily activities and events taking place at the regional office not being recorded and monitored.

At the Thaba Nchu regional office, all research participants **TN 1–10** maintained that the following access control measures are in place: the gate which is used for the entrance and exit of both vehicles, visitors and employees, 24-hour security guards to direct visitors to different offices and a perimeter fence around the premises.

Participants 5, 6 and 2 mentioned the doors to maintain access control in the main building which is occupied by the employees of the regional office from different directorates, including cashiers on the ground floor to collect payments of rates and taxes rates. **Participants 9** and **10** mentioned windows and lastly, **participants 2**, **4** and **8** added the doors to control access into the building and offices.

In Botshabelo, **participants BT 1**–**15** unanimously maintained that the access control measures that are in place in their regional office included private security personnel, gates and the perimeter fence.

In summary, participants in the study confirmed the following access control measures exist at Mangaung Metropolitan Municipality. These include perimeter fence and gates, boom gate, roller door, security guards, doors and CCTV cameras.

Under this theme, all participants in the study acknowledged the presence of access control measures at all three regional offices and they went on to elaborate on the various types of access control measures. These were grouped into categories such as private security guards, perimeter fences and gates, roller doors, windows and

CCTV cameras. The findings concur with Harris' (2016) view who suggests that access control system usually entails a physical access control system that makes use of security barriers such as fences, locks, gates, manholes, mantraps and turnstiles. Fences provide a boundary between the public spaces and the perimeter of the building (Hutter, 2016:2). Fennelly (2013) maintains that gates are significant to facilitate and control access for employees, customers and visitors into the facility. For this purpose, gates always need to be controlled to ensure that only authorised people and vehicles pass through them (Fennelly, 2013:342).

4.3.1.2 Theme 2: Effectiveness of access control measures

To establish the capability of access control measures at the regional offices, all participants were required to indicate whether these were effective. At the Bloemfontein regional office, most of the participants felt access control measures are effective because security is deployed at the entrance of the main building where visitors sign the attendance register which records all their details and the purpose of the visit and the office to be visited. This view is also shared by the participants **BL 15**, **BL 13**, **BL19**, **BL6**, **BL7**, **BL8**, **BL 3**, **BL 4.** In addition, all participants such as **BL1**–**20** indicated that the visitors sign the attendance register that records all their details including the purpose of the visit and officials to be visited.

Participants at the Thaba Nchu regional office provided the following reasons for access control measures being effective:

Participant TN1 They are effective because they can protect people and the building against criminals. This view was shared by **participants TN 10**, **TN7.**

Participant TN 4 maintained that they are partially effective. They are effective now during the Covid-19 lockdown measures because everybody's particulars, including those of employees, are recorded in the attendance register.

At Botshabelo **r**egional office**,** participant **BT 2** felt that they are effective because they are identifying people entering the premises. The fact that there are security guards at the gate is a deterrent against the commission of crimes; **BT 3, 5, 6** and **10** maintained that members of the public are directed to relevant offices within the regional office. **Participant BT 4** said they are partially effective; **Participant BT 1** said that they are trying to regulate access control.

Most of the participants in the study in the three regional offices felt that the access control measures to identify and authenticate visitors were effective and provided reasons for this view. Saflec (2018) maintains that effective access control measures assist to detect security breaches and prevent any unauthorised entry into the premises. In this way, it acts as a deterrent to prevent criminal activity such as theft, vandalism, burglary, and arson (Saflec, 2018:1).

The following categories were extracted from this theme: security officer, visitor's attendance register

Research Question 3: ***What are the reasons for access control measures not being effective?***

4.3.1.3 Theme 3: Reasons for access control measures not being effective

Some participants at the Bloemfontein regional office **BL1**, **BL16** maintained that they are not effective because visitors just sign the attendance register without any form of verification with their identity documents. They expressed concern that there is no tracking of visitors once entering the building. This allows them to move around once freely inside the building. Some use this as an opportunity to enter offices not indicated in the attendance register and consequently steal valuables such as laptops and other personal belongings.

In this study, participants TN 2, 3, 5, 6, 8, 9 indicated that they are not effective because there is no attendance register for people to sign which must record their particulars, no identity documents are requested from the visitor to prove their identity. **Participants TN7 and TN 9** added that employees' belongings are stolen from their offices.

Participant TN5 They are not effective because once people have entered the building, they wander around in the building by going to other offices than those offices indicated to the security that they are visiting. Again, security officers are situated at the entrance to the building instead of at the gate so that vehicles going in and out of the regional office can be searched and people's details and particulars are recorded there. According to **participant TN 5**, they do not record the particulars of people entering the building to pay their rates and taxes and are visiting both the regional manager and the employees.

Participant TN8 They are not effective because security just asks you where you are going and let you in.

Participant TN9 They are not effective because people who are not supposed to be in the building, enter it and this creates a risk that employees may be injured, and property of the municipality stolen.

Research **participants BT 3**, **7**, **8**, **9**, **10**, **11**, **12**, **14** maintained that the failure to operate effective access control is because security does not record the details of the visitors, who are merely asked where they are going and then directed to the relevant building and offices within the regional office. **Participants 2**, **3, 7**, **9**, **12**, **13**, 14 and **15** indicated that there was no proper track record of the visitors on entering the premises since they go to places that they are not entitled or permitted to visit.

According to the research participants, access control measures that are currently in place in the three regional offices are inadequate and ineffective due to the following reason: It is not mandatory for visitors to submit their identity documents in the regional offices to enable the security personnel to validate their particulars against their information that is furnished in the attendance register in the case of Bloemfontein. The situation is worse in Thaba Nchu and Botshabelo with a lack of attendance registers to record the details of visitors. According to Saflec (2018:1), it is important to keep and maintain a proper record of visitors by using the attendance register to provide a detailed electronic visitor history and record through a paper trail that can be inspected to track occurrences within the facilities in the event of security breaches which might lead to loss of life, damage to property and unauthorised removal of organisational assets (Saflec, 2018:1).

Badges and ID cards are common methods of identification for physical access control into the premises. According to Homeland Security (2015: 16), badges bear the holder's photo and personal details together with the name and logo of an organisation. They are useful by providing evidence that the bearers are authorised to be in the premises and buildings of an organisation as well as to prove their identity. These come in the form of smart cards, name tags and identification cards which are integrated with access control systems to allow the validation of individuals (Truett, 2015:99).

Participants further attributed the ineffectiveness of access control to the lack of the patrolling of both the perimeter and interior of the buildings due to inadequate security personnel. Mahambane (2014:10) maintains that security personnel at access control points play a significant role by providing the backing and support necessary for effective access control by providing adequate surveillance and prompt response to mitigate threats to the organisation. Among the roles that they perform are the following: screening employees and visitors in the reception area, controlling access into the facility, inspecting packages and vehicles, issuing visitors with badges for use during the duration of the visit and collecting them before visitors' departure from the premises (Mahambane, 2014:10).

Regional offices do not have a system to monitor visitors once they gained access to the premises and buildings which results in them wandering around the buildings and going into offices that are not indicated in the attendance register in Bloemfontein; nor is information provided to the security officers in the Thaba Nchu and Botshabelo. The result of this anomaly is that criminals steal council property and employees’ belongings. Mahambane (2014:10) maintains that visitors must be escorted to areas that they visit within the premises and building, and their movements must be monitored in all secure areas (Mahambane, 2014: 10).

The three regional offices run the risk of employees and visitors sustaining injuries as a result of dangerous weapons gaining access into the buildings due to lack of metal detectors, no safes to store the weapons of members of the public other than those of the police, traffic officers and the Mangaung Metropolitan Municipality law enforcement officers, a situation which may also place the lives of employees and members of the public in danger. ASIS International (2009) maintains that X-ray machines and metal detectors are used to detect and identify dangerous objects which might endanger the lives of people within the premises. These devices, together with security officers and sniffer dogs, are able to detect contraband brought onto the premises (ASIS International, 2009: 20). According to Lombard (2013), visitors are to be subjected to a metal detector and in the event an alarm is raised, physical searches must be conducted, and access is denied to any suspicious-seeming people (Lombard, 2013:45).

The utilisation of one entrance by the Bloemfontein regional office and the Department of Home Affairs is a risk in itself because patrons of the home affairs park their vehicles on the premises of the regional office and some enter the premises without being documented, because there is no security at the gate to operate access control. Atlas (2013:70) states that the use of security gates is an effective access control measure if it is operated to regulate one entrance into and out of the premises. The benefit from this is that limiting the number of access entry points is an effective way to prevent criminal activities because the more the facility has, the more criminals have easy escape routes. Any other alternative entrance and exit other than through the gates will raise suspicion which will result in detection and ultimately apprehension (Atlas, 2013: 70).

Fennelly (2013:342) maintains that gates are significant in facilitating and controlling access for employees, customers, and visitors into the facility. For this purpose, gates always need to be controlled to ensure that only authorised people and vehicles pass through them (Fennelly, 2013: 342).

Research Question 4: *What are the weaknesses of access control in your regional office*?

4.3.1.4 Theme 4: Weakness in access control system

To try and establish any gaps and inefficiencies of access control measures in the regional offices, the above question was asked, and the following responses were given by the research participants.

Participants BL 7, 3, 9, 15, 19, 5, 2 and 16 maintained that access control measures in the Bloemfontein regional office cannot confine visitors to offices indicated to the security personnel and the attendance register. People wander around the whole building after signing the register at the security other than those offices that they indicate in the attendance register and there is no follow up from security to track their movements once inside the building.

Participants BL 1, 2, 11, 13, 17, 4 and 13 indicated that there is no register for laptops carried by both employees and members of the public when entering and leaving the building which makes it impossible to determine whether those laptops belong to the council or not.

Participants BL 20, **18**, **3**, **6** and **10** indicated that in the regional office, there are no safes for weapons for storage from members of the public which in itself is a security risk for firearms to be allowed into the building without being accounted for. These can be used to harm employees and members of the public.

Participants BL1, 4, 7, 12, 14, 9, 4, 12, 8, 3, 6, 15, 19, 20, 17 raised the concern that there is no form of identification like access cards required from either employees or members of the public when entering the building, to verify their particulars that are required in the attendance register.

Participants BL 3 and **7** indicated that the CCTV cameras do not work, therefore there is no recording and monitoring of events at the regional office.

Participants BL 1–20 maintained that both gates, one from the main entrance and the other from the side of Home Affairs regional office remain open and no security officers manning them.

Participants BL 9, 2, 16, 18, 20, 5, 8, 4, 1, 10, 19, 14, 7 and 3 indicated that the vehicle entrance remains open, no patrols are conducted by security in the premises and inside the building.

Participants BL 3, 9, 20, 4, 11, 7, 12 and 15 indicated that there are no escorts for visitors to different offices nor is confirmation of appointments or visits with employees indicated in the attendance register.

Participants BL 14, 17, 1, 8, 6, 10, 20, 16, 4, 11, 12, 18, 2, 19, 3 and 5 mentioned that the basement parking door is unmanned by the security personnel and the boom gate does not work, the door which sometimes remain open and also unmanned from the hall to the building and no forms of identification requested from members of the community.

Participants BL 9, 19, 15, 3, 10, 13, 7, 11, 16 and 1 raised the concern that there are no metal detectors to identify and search for dangerous weapons from either employees or visitors.

Participants BL 3, 2, 8, 13 and 15 maintained that there is no register to be completed by employees after hours in order to keep a proper track record of their visit for accountability in the vent anything happens to them while inside the building.

Participants BL 1–20 raised the concern of inadequate security personnel in the regional office which could improve the manning of both gates, patrol the perimeter and the interior of the building.

At the Thaba Nchu regional office, **participant TN 2** indicated that there are no weaknesses according to his knowledge.

Participants TN 1–10 responded that there is no proper track record of people entering the building because there is no attendance register to record their details.

Participants TN 1–10 maintained that another weakness of access control is that security guards are only stationed at the entrance to the building and not at the gate to record and take details of visitors before entering the offices.

Participants TN 3, **5**, **6 and10** maintained that there are no metal detectors to search people for dangerous weapons and other contraband, as well as searching of vehicles in and out of the regional office.

Participant TN 7 indicated that there is no guard room and participant **TN3** added that there is no information centre to guide visitors and that **participants 4** and **8** maintained that visitors are not escorted to the office which is a security risk. **Participant 1** indicated that the CCTV in the regional office does not work and therefore can't record events taking place.

Participants TN 1, 2, 3, 4, 8 and 10 indicated that there is a lack of security aids like pepper spray to enable security personnel to protect themselves and no surveillance cameras on the premises and inside the building to record events taking place.

Participants TN 1–10 maintained that there are not sufficient security personnel to conduct effective access control, no policy to guide employees and members of the public about access control measures in the building.

Participants TN1–10 maintained that there are inadequate numbers of security officers and therefore no patrols are taking place inside the building to protect employees and assets: security guards cannot control irate community members visiting the regional office as well as there being an inadequate amount of security personnel.

From the responses recorded from participants in the Botshabelo regional office**, BT 1–15** maintained that there are inadequate security guards, no attendance registers to record the details and particulars of visitors and that visitors are not required to submit their identity documents for verification of their identity. There is no proper record of people entering the regional office; people enter the premises and building unnoticed. **Participants BT 11**, **14** and **15** maintained that there is no escort for visitors going to different departments in the regional office.

Participants BT 2 and **10** indicated that security guards desert the posts to escort the elderly to different buildings in the regional office and this causes the gate to be unmanned with no access control being operated.

Participants BT 2, 3, 4, 7, 8, 9, 10, 11, 13, 15 There are no metal detectors to search for dangerous weapons, vehicles are not searched when they enter and leave the premises.

Participants BT 3, 5, 6, 8, 9, 11, 12, 13 and 15 maintained that the weaknesses of access control in their regional office are that employees are not issued with ID cards to identify them during official working hours. Participants **BT 3** and **BT 7** raised concerns about the lack of cooperation by employees in the implementation of access control.

Participants BT 3, 7, 8, 10, 11 and **13** maintained that there is no attendance register for completion by employees visiting the regional office after hours.

Participant BT 11 maintained that there are no CCTV cameras to monitor and record the movements of people on the premises.

The following categories emerged from this theme: visitors just sign the register without any form of verification, no tracking of visitors once entering the building, no attendance registers, no identity documents required, security officers do not record the particulars of people entering the building, unauthorised people entering the building, lack of patrolling of both the perimeter and interior of the building, dangerous weapons gaining access into the building due to a lack of metal detectors, no safes to store weapons, no register for laptops carried by both employees and members of the public when entering and leaving the building, CCTVs cameras do not work, no security deployed at the gates, no escorting of visitors to different offices, non-functional boom gates, no information centre to guide visitors, lack of security aids, security officers deserting their posts, employees not issued ID cards.

In summary, participants in the study felt that the weaknesses of access control measures in the three regional offices related to the following factors: No identity documents required from the visitors that are then validated against their particulars in the attendance register, which is applied in the Bloemfontein regional office. According to Homeland Security (2015), badges and ID cards are common methods of identification for physical access control at premises. Badges bear the holder's photo and personal details together with the name and logo of an organisation (Homeland Security 2015: 16). They are useful in providing evidence that the bearers are authorised to be on the premises and in the buildings of an organisation as well as to prove their identities. All participants from the regional offices expressed concern about the lack of proper measures to monitor visitors once they have gained access into the premises and offices, something which they felt was a security risk; the identification of employees is a problem because they are not issued with identity cards (Homeland Security 2015: 16).

Furthermore, the following were identified: Inadequate security personnel which made it impossible for both perimeter and interior patrols to deter criminal activity; no metal detectors to identify dangerous weapons that could physically harm both employees and members of the public; no security aids to provide protection to security personnel against irate members of the community and criminals; gates unmanned by security personnel, especially in the Bloemfontein and Thaba Nchu regional offices and that the particulars of visitors in Thaba Nchu and Bloemfontein regional offices are not recorded due the absence of attendance registers. Access control programs are instituted by organisations to permit or deny entry at any given space in order to control the movement in, from and within the premises (Homeland Security, 2015:1). Its main objectives are to protect employees, visitors, property and assets from unauthorised people. To minimise the opportunity to commit crime by preventing and restricting access to assets, computer equipment, operating procedures and other sensitive materials to authorised people only (Baker,2016:98).

Research Question 5: ***How is access control operated for both visitors and employees?***

4.3.1.5 Theme 5: Operation of access control for visitors and employees

In establishing which access control aids or tools were used for both visitors and employees at the three regional offices, the above question was asked, and the following responses were given by the research participants.

In Bloemfontein, participants BL 1–20 indicated that visitors sign the visitor's register which records their details and purpose of their visit, but employees just enter without any form of identification or signing the register except under Covid-19 requirements.

In Thaba Nchu, participants TN 1–10 responded to this question by referring to the two scenarios for visitors and employees in the application of access control as before the Covid-19 lockdown when visitors accessing both the building and the perimeter were not recorded in the attendance register; people would just inform security guards at the gate about the purpose of their visits and subsequently be let in. Employees, on the other hand, will just enter without any form of identification requested. Only during the lockdown were the particulars of both employees and members of the public required and recorded for the screening process.

At the Botshabelo regional office, Participant BT 2 indicated that visitors are scanned for dangerous weapons at the gate, that there is an attendance register to record their details. By contrast, employees do not want to cooperate by signing the attendance register.

Participant BT 15 responded that visitors sign the attendance register which record their details and particulars including the purpose of their visit.

Participants BT 11, 3, 8, 5, 6, 4, 7, 10, 4, 2, 13 and 14 responded that visitors are only asked where they are going, are then just directed there and allowed to go without their particulars being taken or producing their identity documents. There are no access cards for employees. Furthermore, they are merely directed to different buildings that they are visiting in the regional office and no attendance register was kept until now, which they need to sign under the Covid-19 lockdown regulations.

Participants BT 1–15 maintained that there was no application of access control for employees until now, where they are only screened and sanitised.

The following categories were generated from this theme: Before the Covid-19 lockdown, visitors entering buildings were not recorded. Only during the lockdown, a proper record was kept for screening process. There is an attendance register but no access cards for employees.

In summary, participants at the Botshabelo and Thaba Nchu regional offices unanimously maintained that visitors just report to security without their details being recorded and are simply directed without being escorted to different offices and that no record is kept for employees. According to Saflec (2018:1), it is important to keep and maintain a proper record of visitors by using the attendance register, to provide a detailed electronic visitor history and record through a paper trail that can be inspected to track occurrences within the facilities in the event of security breaches which might lead to loss of life, damage to property and unauthorised removal of organisational assets (Saflec, 2018:1).

Research question 5: ***Who are the key players in the implementation of access control in your regional office?***

4.3.1.6 Theme 6: Responsible persons for implementation of access control in your regional office

In establishing an understanding of the stakeholders responsible for the application of access control in each region, the above question was asked, and the following responses were given by the participants:

In Bloemfontein, participants BL1–15 maintained that it is the Regional General Manager, security and law enforcement. **Participants BL 3**, **9** and **10** mentioned facilities management and **participants 3 and 4** added individual employees in the regional office.

In Thaba Nchu, participants **TN 8, 10, 5 and 2** mentioned the law enforcement officers of the Mangaung Metropolitan Municipality to provide oversight to the private security officers; **Participants TN 1**–**10** named the private security officers contracted by the municipality. Participants **TN 10**, **6**, **3**, **2**, **5 and 8** mentioned the regional manager.

Participants TN 8 and **3** indicated that the facility management is a key stakeholder, **participant 1** mentioned the municipality IT department for the maintenance of CCTV are the key stakeholders to implement access control and finally, **research participant TN 3** remarked that employees are major stakeholders in the implementation of access control in the regional office.

Participant TN 6 also said that the municipal employees are important stakeholders in the implementation of access control at their regional office.

However, in Botshabelo**, participants BT1**, **4**, **6**, **8**, **9**, **13**, **11**, **5**, **2** and **14** maintained that the Regional General Manager is responsible for implementing access control at the regional office. **Participants 3**, **8**, **4**, **10** and **13** mentioned municipality law enforcement as a key stakeholder with its responsibility being to maintain oversight of the activities of private security personnel. **Participants BT 1**–**15** designated private security officers.

The main categories emerging from this theme are:

Regional General Manager, security and law enforcement, private security officers contracted by the municipality, IT department.

In summary, on the question of the main stakeholders in the operation of access control in the regional offices, all participants unanimously agreed that they were the regional general managers, Mangaung Metropolitan Municipality law enforcement officers and the private security personnel.

4.4 SECTION C: SECURITY RISKS AND VULNERABILITIES CONFRONTING THE MANGAUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICES AT ACCESS CONTROL POINTS

Research Question 1: ***What are the important assets that need protection at access control points in the regional office?***

4.4.1 Analysis and discussion of findings

4.4.1.1 Theme 7: Protection of assets at access control points in the regional offices

In response to this question, participants BL1-–20 mentioned cash for rates and taxes, employees and members of the public, laptops and computers, municipal vehicles and buildings.

In Thaba Nchu most participants, TN 1–10, mentioned the money safe at the rates and taxes hall,

Participants TN 1–10 indicated furniture, employees, municipal vehicles, buildings and members of the public.

Participants TN 6, 10, 2, 5, 3, 8 and 9 mentioned the following assets: laptops and desktop computers.

Participants BT 1–15 indicated that vehicles and machines, desktop computers and laptops, employees, members of the public, buildings and offices are the most important assets in the regional office.

Participants BT 11 and 9 also added firearms that are stored in the safes at the regional office for both traffic and law enforcement officers of the Thaba Nchu regional office.

The categories that were generated from this theme are the following: cash in rates and taxes, employees and members of the public, laptops and desktop computers, vehicles and buildings, furniture and firearms.

In summary, the research participants mentioned the following assets that need maximum protection at their regional offices: cash from rates and taxes, firearms that are stored in Botshabelo regional office for use by traffic and law enforcement offices of both Thaba Nchu and Botshabelo regional offices, municipality vehicles and machinery, desktop computers and laptops, furniture, employees and visitors. Access control is therefore an element of physical security to ensure the protection of premises and their assets (British Security Industry Association, 2016:14).

Research Question 2: ***What security risks are at access control points in your regional office?***

In establishing current security risks at the regional offices access control points, the participants were asked the question above and the following responses were received.

4.4.1.2 Theme 8: Common security risks at access control points

In the Bloemfontein regional office participants 2, 6, 9, 5, 20, 19, 13, 17, 11, 8 felt that physical harm was one of the risks at access control points due to angry and violent members of the community during service delivery protests and because of people's frustration with rates and taxes.

Participants BL 1–20 mentioned heists of cash-in-transit vehicles collecting money from the rates and taxes office to be transported to the bank, including the income from the home affairs regional office next to the regional office, theft of council property, burglary at the offices and intimidation during service delivery protests.

In Thaba Nchu**, participants TN 1–10** mentioned the following risks that are found at access control points: Angry community members protesting the lack of services, theft and robbery resulting from attacks on cash-in-transit vehicles collecting money from rates and taxes that need to be banked, theft of municipality property because vehicles are not searched and there is no policy for the removal of laptops, regarding undocumented and unidentified people, the intimidation of both employees and security personnel by members of the community during service delivery protests.

Participants TN 2, 7 and 9 raised a concern about unauthorised entry since members of the public just enter without being noticed by security personnel which places both employees and members of the public in great danger.

Participants TN 6, 10, 7, 2, 4 and 8 mentioned service delivery protests by members of the community and vehicles impounded by the traffic department that are parked at the regional office, increasing the risk of burglary and theft.

At the Botshabelo regional office**, participants BT 1**–**15** mentioned **the** theft of assets, safety of employees and vehicles.

Participant BT 7 mentioned heists.

Participant BT 4 indicated theft, bodily harm for both employees and visitors.

Participants BT 6 ,**10, 4, 3** pointed out the burglary of the stored firearms of traffic and security officers.

Participants BT 9, 13, 11, 1, 3, 5, 7, 10, 14 and 6 remarked on potential injury to employees and members of the community during service delivery protests.

Participant BT 8 indicated ineffective access control and theft.

Participants BT 1–15 mentioned marches and protests, injury to employees, damage to property, bombing of people and theft.

Categories that were generated from this theme are the following: physical harm during service delivery protests, heist of cash-in-transit vehicles after collecting money from the rates and taxes hall, theft because vehicles are not being searched, no policy for the movement of laptops and undocumented and unidentified people.

The majority of employees in the three regional offices maintained that security risks and breaches at access control points were physical injury to employees, members of the community and security personnel; theft of council property and personal belongings of employees; heist of cash-in-transit vehicles collecting council income from rates and taxes; burglary and intimidation of both employees and security personnel during service delivery protests by the members of the community. According to Marozas (2013: np), the aim of access control is to prevent security breaches by monitoring and regulating the movement of people in and out of the facility by allowing those that are permitted and denying entrance to unauthorised people.

In determining the perpetrators of these security breaches, all participants maintained that they were members of the community, criminal elements and to a certain extent, employees.

Research Question 3: ***How vulnerable are employees, visitors and contractors in the premises of the municipality***?

4.4.1.3 Theme 9: Vulnerability of employees, visitors and contractors in the premises of the municipality

In establishing the level of exposure to danger by employees and visitors at the regional offices, the question above was asked and the following responses were recorded.

Participants BL 1–20 maintained that they are vulnerable as a result of gaps in the access control system at their regional office.

Participants TN1–10 (which is 100% of the responses by participants) maintained that they are vulnerable because members of the community and those likely to pose a threat to the regional office can enter and cause injury without being authorised, identified, searched and noticed.

Most of the participants in Botshabelo BT1–15 maintained that they are vulnerable and in danger of attacks by criminals and members of the community.

The following categories are extracted from this theme: members of the community can enter the building and cause injury without being authorised, identified, searched and noticed.

Research Question 4: ***What security breaches relating to access control normally occur at access control points?***

4.4.1.4 Theme 10: Security breaches relating to access control

In establishing the nature of incidents related to security at the regional office, the question above was asked and the following responses were recorded:

Participant BL 17 mentioned unaccompanied and unauthorised access into the building.

Participant BL1–20 identified the theft of desktop computers and laptops, attempted cash-in-transit heists, burglary and hostage-taking of employees and security, community service delivery protests, assaults of security personnel and intimidation of employees and security personnel by members of the community.

Participants TN1–10 indicated employees not cooperating with security, attacks on security guards by the members of the public, attempted heists of cash-in-transit vehicles collected money from the rates and taxes hall, the theft of laptops and unauthorised people entering the premises and buildings.

Participants BT1–15 specified theft, assault on security officers by angry members of the community and the unauthorised entry by people.

The following categories are found from this theme: unaccompanied and unauthorised access of visitors into the building, theft of desktop computers and laptops, attempted cash-in-transit heists, burglary, hostage-taking of employees and security during community service delivery protests, assault on security officers by angry members of the community.

Research Question 5: ***Who are the perpetrators of these breaches relating to access control at your regional office*.**

4.4.1.5 Theme 11: Perpetrators of security breaches relating to access control

In establishing the identity and profile of people committing these security acts, the questions above were asked and the following responses were received:

Participants BL 1–20 felt that they are members of the community, employees, people using the hall for events and home affairs employees and visitors.

Participants TN 1–10 suggested that these breaches were committed by the employees, criminals and irate members of the community due to service delivery issues.

Participants BT1–15 stated that the perpetrators are members of the community as well as criminals.

The following categories were generated from this theme: members of the community, employees, and criminals.

On the determination of the extent of vulnerability that employees and members of the community can be exposed to, all the participants in the regional offices responded in the affirmative.

The three regional offices are vulnerable due to their probable exposure to security risks such as theft, armed robbery and cash-in-transit heists of council income from rates in taxes, intimidation and physical harm to both employees, security personnel and visitors by members of the community during service delivery protests. Saflec (2018) maintains that access control measures provide protection for employees and other lawful stakeholders within the premises against any physical harm and injuries (Saflec, 2018:1).

The security officers are vulnerable due to the lack of security aids to protect themselves against angry members of the community and criminals and this increases the probability of them being harmed. Kole (2013) maintains that security officials should be provided with the following security aids when they are on duty: whistles to alert and request for assistance in the event of an emergency, baton sticks to protect themselves against attackers, firearms for protection in more violent areas and lastly, handcuffs to apprehend suspects (Kole, 2013:13).

4.5 SECTION D: TYPES OF ACCESS CONTROL MEASURES TO BE IMPLEMENTED IN THE REGIONAL OFFICE

Research Question 1: ***Which security measures must your regional office implement to manage access control?***

4.5.1 Analysis and discussion of findings

4.5.1.1 Theme 12: Types of access control measures to be implemented in the regional offices

In establishing recommended access control measures at the regional offices, the question above was asked and the following responses were recorded:

In the Bloemfontein regional office, most of the participants, **BL 20, 13, 6, 9, 13, 15, 3, 18, 19, 1** proposed that CCTV cameras should be installed so that all activities taking place in the regional office can be recorded and monitored.

Participants BL 3 and **6** recommended that turnstiles are installed at the entrance of the main building.

Participants BL 1–20 suggested for biometric finger scanning to be installed at the entrance of both the main building and the rates hall.

Participants BL1–20 submitted that metal detectors should search both visitors and vehicles entering the premises and building.

Participants BL17, 8 and **14** proposed that employees coming to the office after hours must sign an attendance register so that the security personnel can have a record of people entering and leaving the building.

Participants BL 4, 16, 12, 7, 10, 11, 1, 5, 8, 13, 15, 17, 9, 14, 20 and**19** stated that employees must be issued ID cards to identify themselves with when entering the building.

Participants BL 1 and 11 suggested electronic access control in the basement parking and that the door from the hall into the main building should be closed to prevent unauthorised and unidentified people from gaining access to the building.

Participants BL 1–20 recommended an increase in the number of security personnel security to patrol the visitors parking area, the perimeter and the interior of the building—to identify unauthorised people.

Participants BL 6, 8, 2, 13, 17, 9, 11, 15, 17, 20, 13, 7 and 4 proposed that security personnel must be provided with aids like pepper spray to protect themselves against irate members of the community during service delivery protests.

Participants BL 7, **17, 15, 3, 10, 12, 9, 20, 18, 13, 3, 5, 11, 16** and **2** put forward a register to record laptops brought in and out of the building by both employees and visitors to ensure that organisational laptops are not stolen by members of the public who loiter inside the building.

Participants 3 and 8 advocated for regular maintenance and patrol of the perimeter fence to ensure that it is not damaged and to prevent unauthorised entrance onto the premises.

Participants BL 1–20 proposed that metal detectors are used for both employees and visitors to search for dangerous weapons and other contraband that might endanger the lives of both employees and members of the community.

Participants BL 10, 16, 3, 9, 17 and 8 proposed that both gates should regularly be closed and opened by security personnel in order to control access into the premises of the regional office.

Participants BL 1, 4, 2, 19, 15, 6, 10, 12 and **16** submitted that all visitors to the main building which houses employees of the regional office should be escorted or that security should call employees to fetch them at the entrance.

Moreover, research **participants TN 2 ,4, 5, 7, 8, 9, 10** and **6** proposed the repair and maintenance of cameras that are not operational; research **participants TN 1–**

10 put forward proper identification of employees through the issue of ID cards and **TN 1–10** proposed the introduction of an attendance register to record the particulars of visitors. All the participants advocated for the use of a biometric system for fingerprint scanning of employees at the regional office. **Participants TN 1–10** felt that access control should be conducted at the gate by security officers. **Participants TN 4 , 7, 8, 9** and **10** advised that all visitors to various offices should be escorted. **Participants 1, 3** and **8** felt that the interior of the regional office should be constantly patrolled by security officers. **Participant TN 5** maintained that the regional office should have an access control policy that must be communicated to both employees and visitors.

In Botshabelo, research participants **BT 1–15** suggested the installation of a biometric finger scanning device for employees**. Participants BT 1–15** maintained that the number of security officers must be increased**. Participants BT 1, 4, 7, 9, 13, 12, 10, 2, 6, 5, 13, 14 and 11** asserted that access control should be conducted at each office block at the regional office. **Participants BT 9, 4, 10, 3, 2, 7, 8 and 10** contended that cameras should be installed inside every office block, to monitor the movements of visitors. **Participants BT 1–15** suggested the use of an attendance register to record the details of all visitors. **Participants BT 2, 7, 5, 6, 10, 4, 5, 9 and 3** proposed the introduction of a register for laptops that must be signed upon entrance and exit. **Participant BT 15** submitted that visitors' vehicles must park outside the premises of the regional office and that only employee vehicles should be allowed to park inside the premises. **Participants BT 1–15** called for the use of metal detectors to search visitors for dangerous object that might harm employees and members of the public visiting the regional office. **Participants BT 1–15** suggested the deployment of security guards at all the gates of the regional office to control access. Participant **BT 3** proposed that two gates must be used: one for entrance and the other for exit. **Participants BT 6 and 9** proposed that the regional office should have an enquiry office which will be used to direct all visitors after confirmation of the appointment and purpose of the visit, with the respective officials.

The following categories were generated from this theme: CCTV cameras to be installed, turnstiles to be installed at the entrance of the building, biometric finger scanning to be installed at the entrance of the main building and rate hall, metal detectors to search visitors and employees, attendance register to record the details of visitors, ID cards for employees, increasing the number of security personnel, a laptop register for both employees and visitors, regular perimeter patrols and maintenance of the fence, escorting visitors into the buildings, conducting access control at the gate and visitors' vehicles to be parked outside.

The research participants felt that the following access control measures needed to be implemented in order to monitor and authenticate visitors and employees in the regional offices: the installation of closed-circuit television (CCTV) to record events on a 24-hour basis. It has been established that the implementation of an access control system is effective when it is integrated with other security aids such as closed-circuit television that monitor and record activities (CCTV) as well as an alarm system that sends a signal during unauthorised entrance into the premises (Umbrella Technologies, 2019:11).

Additionally, closed-circuit television should be used in areas 24/7 from a central location to monitor the perimeter, including areas that might be obscured from guards (Rao, 2016:66). According to Fennelly (2012:262), the CCTV cameras should also be installed at access control points to monitor and record access into, within and outside of the facility. Rao, (2016) maintains that although CCTVs are effective in monitoring movements, it is a passive device that can only monitor the intrusion but cannot prevent it and must be integrated with other security measures in order to be effective (Rao,2016:66).

The Issuing of ID cards to employees for easy identification by the security officers is also necessary. According to the American Government’s Homeland Security (2015), badges and ID cards are common methods of identification for physical access control into premises; badges bear the holder’s photo and personal details together with the name and logo of an organisation. They are useful in providing evidence that the bearers are authorised to be in the premises and buildings of an organisation as well as to prove their identity (Homeland Security, 2015:16).

Participants felt that attendance registers should be introduced at the Thaba Nchu and Botshabelo regional offices and the Thaba Nchu and Bloemfontein regional offices; security officers should maintain access control at the gates. This, according to Moses (2016), will assist the regional offices during the auditing process in monitoring the effectiveness of the access control system by maintaining an audit trail that keeps a record of all previous access movements and activities within the premises (Moses, 2016: 669).

The dysfunctional boom gate at the basement parking of the Bloemfontein regional office must be repaired or manned by a security guard to prevent unauthorised access into the main building by criminal elements. The use of security gates has proven to be in effective measure to reduce theft and burglaries in facilities. According to Rhodes (2020:np), gates are a common method to restrict vehicle and pedestrian access to premises and properties. For the gate to be effective, it needs to be integrated with other security measures (Rhodes 2020: n.p.).

The number of security guards to patrol both the perimeter and the interior of the buildings must be increased. Mahambane (2014:10) maintains that security personnel at access control points play a significant role by providing the backing and support necessary for effective access control through adequate surveillance and prompt response to mitigate threats that can harm the organisation. Among the roles that they can perform are: the screening of employees and visitors in the reception area, controlling access to the facility at other points, escorting visitors, inspecting packages and vehicles, issuing visitors with badges for use during the duration of their visits and collected before departure from the premises and finally, monitoring the movement of employees and visitors in secure areas (Mahambane, 2014:10).

The application of biometric technology in the three regional offices, similar to the Bram Fischer building (the head office of the Mangaung Metropolitan municipality) is needed. Biometric access control is a system that helps to prevent unauthorised individuals from accessing facilities and includes physical access control measure and logical access control based on biometric authentication (Thales, 2020: n.p.). The application of biometrics to recognise people is derived from images of fingerprints, hand vein patterns, retinas, irises, facial expressions, signatures, voice patterns and body temperature to authorise access to the premises (Norman, 2017: n.p.).

Repairing the keypad in the Bloemfontein regional office for use by employees. Keypads are a common and reliable method of access control that consists of unique codes known as a personal access code (PAC) or personal identification number (PIN). They are ID readers that contain several digits known to the authorised user to gain access into the perimeter or building (Niles, 2011:8). Norman (2012:52) argues that they are relatively cheap and easy to use but vulnerable to duplication in the event that an authorised person gets to know the code.

Participants at the regional offices felt strongly about the introduction of turnstiles at the entrances of the buildings. According to Homeland Security (2015:13), turnstiles are security barriers used to restrict and manage human traffic flow at access control points. Turnstiles can be used as the main method of access control in a lobby or in combination with access control at other exits and entrances by permitting exit without the use of the access control system while entering is only at an access control entrance (British Security Industry Association, 2016:35).

Similarly, Baker (2016:106) maintains that turnstiles are regarded as a supplementary access control measure to assist both the guards and receptionist whilst controlling access into a protected area (Baker, 2016:106). Turnstiles are valuable in preventing tailgating which is a situation where an authorised person facilitates the entrance of an unauthorised and unverified person (Homeland Security, 2015: 13).

Research Question 2: ***What access control measures should be implemented to monitor and detect unauthorised entry of people into the premises of the regional office?***

4.5.1.2 Theme 13: Types of access control measures to be implemented to monitor and detect unauthorised entry of people into the premises of the regional office

At the Bloemfontein regional office, participants **BL 4, 2, 16, 20, 19, 13, 11, 17, 3, 9, 8, 12, 15, 13** believed that closed-circuit television (CCTV) should be installed at the regional office to monitor and detect unauthorised people inside the premises and buildings**. Participants BL 5 and 6** suggested the installation of alarms system to detect unauthorised entry. **Participants BL 1–20** proposed that it should be mandatory for all visitors to the regional office to produce ID documents that verify their identity against information entered into the attendance register**.**

Concurrently, at Thaba Nchu, the research **participants TN 1–10** maintained that the closed-circuit television is obsolete and must be repaired and maintained to record the movement of people on the premises, an attendance register to record the details and particulars of visitors is needed and that access control should be maintained at the gate rather than the entrance to the building. **Participants TN 3, 8, 5, 7 and 2** suggested that employees in the regional office must be issued with ID cards that bear their photos and names in order to be identified by security officers.

Similarly, in Botshabelo, participants BT 1–15 proposed that the number of guards should be increased so that they could be deployed at the entrance of each building block to control access, patrol the premises and to control access at the other two gates.

Participants BT 2 and 4 proposed that the closed-circuit television (CCTV) be installed at the entrance of each building to monitor and record the movement of people.

Participant BT 6 felt that an access control policy should be compiled and communicated to both employees and visitors.

Participants BT 1–15 proposed that metal detectors should be made available to search people for dangerous weapons that can endanger the lives of employees.

Participants BT 1, 2, 4 and 6 proposed that employees as well as visitors be issued with ID cards and that visitors must sign an attendance register and submit personal identity documents for verification when visiting the regional office.

Participant BT 5 suggested that gates should be closed, and security officers should be issued with pepper spray and panic buttons to protect themselves in the event of being attacked.

Participant BT 8 suggested the reduction of the number of access points and an increase in the number of security personnel, so that they can patrol the interior of the buildings to protect employees and visitors; the establishment of an enquiry office when visits can be confirmed with responsible officials to prevent people from roaming around the buildings. Finally, all visitors must be escorted to the offices that they are visiting as well as the application of a biometric system like at the head office of the municipality.

Participant BT 3 proposed that all gates in the regional office always be manned by security officers.

Participant BT 1 proposed erecting guard rooms at all the gates.

Participant BT 11 felt that all municipal and employee vehicles should be allowed on the premises and that visitors' vehicles must be parked outside.

The following categories were generated from this theme: Guard room to be erected at all gates, all gates to be manned by the security officers, security officers to be issued with aids to protect themselves, the number of gates to be minimised, visitors to be escorted to offices, biometric system to be installed at entrances, regular exterior and interior patrols by security officers, metal detectors to be made available to search for dangerous objects, access control policy to be communicated to both employees and visitors, CCTV cameras to be installed.

Research Question 3: ***How could access control be improved in the future to ensure the safety of property, assets, employees and visitors at the regional office?***

4.5.1.3 Theme 14: Measures to improve access control

In establishing future improvements of access control measures in the regional offices, the above question was asked, and the following responses were recorded:

BL 6, 17 and 9 believed that the keypad being used by employees to gain access to the main building should be repaired for access control. **Participants BL 1, 3, 6, 9, 11, 7, 16, 14, 20, 10, 18 and 13** felt strongly that there should be a security officer at the entrance of the basement to control access and conduct patrols inside the basement. **Research participants 9, 2, 13, 12, 14, 20, 6, 3, 17**, **19, 16, 15, 7, 4, 8 and 3** thought that security officers should conduct patrols inside the buildings to monitor and control the movement of people and identify those wandering around offices other than what is indicated in the attendance register. **Participants 1, 15, 4 and 19** believed that all members in the regional office should carry identity cards that bear their pictures and names for identification purposes when inside the premises and buildings. **Participants 1, 2, 7, 8, 11, 3 and 20** felt that a biometric finger scanning system like that being used at the head office in Bram Fischer building, should be installed at the entrance of the building including the basement parking for all employees of the regional office. **Participants 7, 13, 17, 16, 11, 9, 5, 19, 17, 3, 20, 10, 12, 14, 6, 2 and 4** strongly believed that a metal detector should be used to search visitors for dangerous weapons that may cause harm to employees and members of the public. **Participants BL 1–20** maintained that all gates at the regional office, one on the site of residences and another from the home affairs regional office should be manned by security officers. **Research participants BL 1 and 2** asserted that employees visiting the regional office after hours should sign an attendance register.

Participants TN 1–10 maintained that security guards should be stationed at the gate, there should be an information desk to provide members of the public with information, the latter must be escorted into the building and for every visit to be confirmed with the official to be visited, that both visitors and employees be issued with ID cards so that they can be identified by both security personnel and employees.

Participants BT1–15 from the Botshabelo regional office felt that since the regional office has a number of buildings occupied by employees from different directorates, it is necessary for access control to be applied at each office block. **Participants BT 1–15** maintained that visitors need to sign the attendance register to record their details at both gates as well as at the entrance of each office block occupied by employees from different directorates. **Participants BT 6, 3 and 14** believed that closed-circuit television (CCTV) that covers the business around Botshabelo and Thaba Nchu area and are manned by the municipality's law enforcement officers must be installed and also used for monitoring the perimeter and entrance to the office blocks, especially where the firearms for both traffic and law enforcement officers in Botshabelo and Thaba Nchu are stored. **Participants BT 9, 11, 6 and 1** felt that visitors must be escorted to the different offices in the regional office.

The following categories were generated from this theme: keypad should be repaired, security officers to conduct patrols inside the buildings, members of the regional office should carry identity cards, biometric scanning to be installed, metal detectors to be used to search for dangerous weapons, security officers should be stationed at the gates.

On the future improvements of access control in the regional offices, the participants mentioned the security measure of biometric scanning. Harris (2013) maintains that this technology is widely used by both government and private organisations worldwide to maintain both physical and logical access control for buildings and premises and as well as highly secured areas like servers and computer systems points. The purpose is to prevent both identity fraud and security breaches in these areas (Harris, 2013:259). Another suggestion was the installation of metal detectors to scan for dangerous weapons. This security measure consists of X-ray machines and metal detectors used to detect and identify dangerous objects that might endanger the lives of people within the premises. These devices are used together with security officers and sniffer dogs, important in detecting contraband brought onto the premises (ASIS International, 2009:20).

The issuing of ID cards and badges to employees for easy identification by the security officers: According to the American Government Homeland Security (2015), badges and ID cards are common methods of identification for physical access control into premises. Badges bear the holder's photo and personal details together with the name and logo of an organisation. They are useful in providing evidence that the bearers are authorised to be in the premises and buildings of an organisation as well as to prove their identity (Homeland Security, 2015:16).

The installation of closed-circuit television (CCTV) to monitor and record daily activities: Rao (2016) maintains that closed-circuit television must operate in areas 24/7 from a central location, to monitor the perimeter including areas that might be obscured from guards (Rao,2016:66). According to Fennelly (2012:262), CCTV cameras are also installed at access control points to monitor and record access into, within and outside the facility.

Increased security personnel to conduct both perimeter and interior patrols to deter crime and unlawful activities, as well as to man the gates in order to implement access control: Mahambane (2014), contends that security personnel at access control points provide backing and support necessary for effective access control. This is because they are on the ground and can provide adequate surveillance and prompt response to mitigate threats that can harm the organisation (Mahambane, 2014:10).

The participants in the three regional officers also felt it should be mandatory for visitors to submit their identity documents in order for security personnel to validate their particulars against the information that they provide in the attendance register; manning of the gates by the security personnel to control access in the premises was also mentioned.

4.6 CONCLUSION

Based on the above study, the following conclusions are made by the researcher regarding the effectiveness of access control in the three regional offices of the Mangaung Metropolitan Municipality.

The three regional offices are vulnerable due to their probable exposure to security risks such as theft, armed robbery and cash-in-transit heists of council income from rates in taxes: intimidation and physical harm to both employees, security personnel and members of the community during service delivery protests.

Access control measures that are currently in place in the three regional offices are inadequate and ineffective due to the following weaknesses: There is no proper measure to identify and authenticate visitors to the regional offices due to the absence of attendance registers at Thaba Nchu and Botshabelo; in the Bloemfontein regional office it is not mandatory for visitors to submit their identity documents for security personnel to validate their particulars against the information that is furnished in the attendance register; there is no proper and effective access control due to a lack of patrolling of both the perimeter and interior of the buildings as a result of an inadequate amount of security personnel.

Regional offices do not have a system to monitors visitors once they have gained access to the premises and buildings which results in them wandering around the buildings and going into offices that are not indicated in the attendance register in Bloemfontein or part of the information provided to the security officers in Thaba Nchu and Botshabelo. The result of this anomaly is that visitors steal council property and employees' belongings.

The three regional offices run the risk of dangerous weapons being brought into the buildings due to a lack of metal detectors, safes to store the weapons of members of the public other than police, traffic officers and the Mangaung Metropolitan Municipality law enforcement officers, a situation that can endanger the lives of employees and members of the public.

The security officers are vulnerable due to a lack of security aids to protect themselves against angry members of the community and criminals; this increases the probability of them being harmed.

The utilisation of one entrance by the Bloemfontein regional office and the Department of Home Affairs is a risk in itself because patrons of home affairs park their vehicles on the premises of the regional office, and some enter the premises without being documented because there is no security at the gate to operate access control.

The absence of security personnel and the non-functional boom gate at basement parking of the Bloemfontein regional office is a serious concern because it can provide an opportunity for unauthorised access to the main building by criminal elements and cause harm to employees and members of the public as well as the theft of council property.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter outlines the conclusion of the research, makes recommendations emanating from the findings of the study and suggests areas to be explored by future research. This study focused on evaluating the effectiveness of access control measures within the Mangaung Metropolitan Municipality regional offices. To achieve these objectives, a qualitative research approach was used to examine the effectiveness of the existing access control measures currently in place within the three regional offices. The researcher used an interview schedule consisting of open-ended questions to explore the participants' perceptions, knowledge and experience of the effectiveness of the existing access control measures within the Mangaung Metropolitan Municipality regional offices.

The study was conducted to provide answers to the following research questions: what existing access control measures currently in place at Mangaung Metropolitan Municipality regional office? What risks are confronting these regional offices as a result of ineffective and a lack of access control measures? Lastly, what future access control measures are recommended to eliminate security breaches within the Mangaung Metropolitan Municipality regional offices?

Based on the research questions, several themes were developed during the data analysis, amongst others the awareness of access control measures. The study found that the majority of research participants in the three regional offices felt existing access control measures to identify and authenticate visitors were not effective and provided a number of reasons to substantiate their claims.

Participants are unanimous that there are gaps and weaknesses impacting the effective application of access control measures at the three regional offices, with a few additions being specific to each regional office. The conclusion by this researcher is that improvements are needed to ensure that access control measures are effective in addressing the unique conditions at the three regional offices.

Participants indicated that there are different applications of access control measures for employees and visitors at the regional offices. The majority of the participants agree that the assets of the municipality are not adequately protected by existing access control measures.

The study revealed that most participants felt very strong about the possibility of security risks that can cause grievous bodily harm to both employees and visitors as well as damage to the property of the municipality at the three regional offices. This highlighted the vulnerability levels of employees, visitors, and contractors in the premises of the three regional offices and confirms the probable exposure of these stakeholders to threats and vulnerabilities.

Most research participants felt that an integrated system comprising physical, electronic, administrative and biometric access control measures is necessary to ensure maximum protection of assets and resources at the three regional offices.

Based on the findings of the study, the following recommendations are proposed:

5.2 RECOMMENDATIONS

The Mangaung Metropolitan Municipality has offices that are spread across a vast geographical area which make them vulnerable to crime. In an effort to minimise the risk associated with poorly implemented access control measures, the researcher makes the following recommendations to improve existing physical access control measures at Mangaung Metropolitan Municipality:

5.2.1 Physical access control measures

- The number of security personnel to be increased to enable them to patrol the perimeter and interior of the buildings to deter and prevent unauthorised access and to protect staff and visitors in the premises of the regional offices.
- The rotation of security officers should be applied in order to discourage familiarity between them and the regional offices employees, which may result in collusion to commit crimes against the municipality and the visitors.

- Turnstiles to be erected at the entrance of the three regional offices to control and manage the inflow of people entering the buildings.
- Security personnel to be capacitated by providing them with security aids such as batons and pepper spray for self-protection against violent members of the community and criminals.
- Mantrap doors to be installed at the entrances of the main buildings of the Bloemfontein and Thaba Nchu Regional offices. In the Botshabelo regional offices, these should be installed in each office block on the premises.
- The boom gate of the underground parking garage in the Bloemfontein regional office should be repaired or alternatively, a security guard must be deployed to control access in order to restrict unauthorised entry into the building.

5.2.2 Electronic access control measures

- The keypad that is non-functional at the Bloemfontein regional office must be activated to facilitate employees' entrance into the main building.
- Alarm systems should be installed in the buildings of the regional offices and be backed by a 24-hour armed response that must be provided by the Mangaung Metropolitan Municipality law enforcement reaction unit and contracted private security companies.
- Metal detectors should be used to search for dangerous weapons and other contraband that may cause physical harm to employees and members of the public on the premises of the regional offices. Mangaung Metropolitan Municipality law enforcement must provide safes for weapons carried by employees and members of the public, to ensure that no one enters the building of the regional offices with a weapon other than the police, traffic- and law enforcement officers.
- The Mangaung Metropolitan Municipality should install closed-circuit television (CCTV) at strategic points such as the entrance, exit points, interior of the buildings and parking areas of the three regional offices—to monitor and record daily events within the perimeter. These must be manned and operated by competent and well-trained security personnel.

- Biometric security system to be installed at the regional offices to authenticate and identify people entering the building and prevent those whose credentials are not stored in the data base.

5.2.3 Vehicle access control

- All visitors’ vehicles must be parked outside the Thaba Nchu and Botshabelo regional offices' premises.
- To control vehicle traffic at the Thaba Nchu and Botshabelo regional offices, two gates should be installed, one for the entrance to the premises and the other to exit.
- Impounded vehicles that are parked at Thaba Nchu premises must be removed because they encourage the theft of spares and in the end, burglary of the municipality's building.

5.2.4 Personnel access control

- All employees at the regional offices must be provided with an ID card bearing their photos and names so that they can be easily identified by the security officers.
- Employees and visitors must complete laptop registers that will record the serial numbers daily to minimise the theft of municipality's laptops.
- All visitors should be required to produce their identity documents in order to enable the security personnel to validate and confirm their particulars against what had been furnished in the attendance register.
- Visitors must be issued with visitors’ cards that must be carried while on the premises of the regional office and be returned to the security officers when they leave the buildings and premises.
- All visitors must be escorted to various offices or alternatively, their visits should be confirmed with officials who must come and fetch them from the reception area. This must be complimented by issuing visitors with pass slips

that have to be signed by the official at the end of the visit and handed over to security personnel upon exiting the building.

5.2.5 Administrative access control measures

- The Mangaung Metropolitan Municipality's law enforcement unit should formulate and develop an access control policy that must be communicated to employees, visitors and security personnel.
- The Mangaung Metropolitan Municipality law enforcement officers must conduct regular oversight and inspection of private security personnel to ensure that they provide effective access control at the regional offices.
- Regular security surveys should be conducted to determine weaknesses and excesses in the access control measures within the three regional offices of the Mangaung Metropolitan Municipality.
- All regional offices must use the attendance registers to record the particulars of every person visiting the regional offices.

5.2.6 Maintenance and management

The Mangaung Metropolitan Municipality‘s regional offices require high-quality, cared-for properties to encourage the respect that will deter potential perpetrators by creating a sense that the premises are always under surveillance and that any attempt to breach the security will lead to apprehension.

5.3 SUGGESTIONS FOR FURTHER RESEARCH

The researcher recommends that further research be conducted on the following aspects:

- Client satisfaction with the aspects of access control should be extended to include the members of the community who visit municipality buildings daily, to solicit their perceptions, feelings and experiences of the effectiveness of access control in these buildings.

- The implementation of a standard and uniform system for access control at all buildings and premises of the Mangaung Metropolitan Municipality.
- Assess the total effectiveness of physical security at all government offices, not only one aspect such as access control.

5.4 CONCLUSION

The study confirmed that a number of different crimes and security breaches occur at the regional offices of the Mangaung Metropolitan Municipality, despite the application of access control measures in the premises and buildings. Access control is a complex phenomenon that must be continually evaluated to ensure its effectiveness in protecting employees and visitors and to mitigate the losses sustained by the municipality through criminal and unlawful activities. Therefore, the recommendations proposed may assist provincial government during the development or updating of the current security policy. Hence, this study makes a modest contribution by pointing out several weaknesses existing in the current access control systems at the various regional offices and this contributes to increase in crime at the Mangaung Metropolitan Municipality offices.

LIST OF REFERENCES

Alexandrou, A. 2018. *Physical security: Interior applications- Doors, Access Control*. In: Shapiro L., Mara MH (eds). Encyclopaedia of Security and Emergency Management. Springer, Cham.https://doi.org/10.1007/978-3-319-69891-5-41-2.

Antron Security.2021. *Rule based access control -What is it?* April:15.

Arifin, SR.2018. *Ethical consideration in qualitative study*. International Journal of Care Scholars, 1(2), 30-33.

Ashburn, J. 2014. *Biometrics. Advanced Identity Verification. The complete guide*, Springer-Verlag. London.2000.

ASIS International, 2009. *Facilities physical security measures guidelines*.

Atlam, H.F.; Alassafi, M.O.; Alshdadi, A.A. & Azad, M.A. 2017. *Risk-based access control model.* A systematic literature review. DOI 10.3390/fi/2060103. University of Southhampton.

Atlas, R.L. 2008. *21 Century security and CPTED: Designing for critical infrastructure protection and crime prevention*. United States of America: Washington DC. Taylor and Francis group, LLC.

Babbie, E. & Mouton, J. 2001. *The practice of social research*. Cape Town: Oxford University Press.

Bairagi,V & Munot, MV.2019. *Research methodology: A practical and scientific approach*. CRC Press. Taylor & Francis Group, Boca Raton, London New York.

Baker, P.R. & D.J. Benny.2016 *The complete guide to physical security.* CRC Press. Taylor & Francis Group, Boca Raton, London New York.

Blaire, T. 2016. *Write a graduate thesis and dissertation.* Volume 4. Rotterdam: Sense Publishers.

Bless, C. 1995. *Fundamentals of social research methods*: *An African Perspective*.2nd edition. Lansdowne: Juta.

Boukhonine, S., Krotov, V. & Rupert, B. 2005. *Future security approaches and biometric.* Communication of the Association of Information System: Vol 16, Article 48. University of Houston.

Bowers, D.M. 1988. *Access control and personal identification systems*, Boston: Butterworths.

British Information Security Association. 2016. *A specifier's guide to access control system.*

Burges, D. 2013. *Cargo theft*, *loss prevention and supply chain security.* Butterworth- Heinemann*.*

Carbric, M. 2015. *Corporate security management. Challenges, Risks and Strategies*. Butterworth- Heineman. Amsterdam- Boston-Heidelberg London. Elsevier Inc.

Caputo, C. 2010 *Digital video surveillance and security*. Burlington- Butterworth-Heinemann.

Chapa, L. 2019. *Assessing federal facilities.* Security Management*,* ASIS International*.*

Chapple, J.M. 2012. *Access control*. Certified information security system professional study guide. John Willey &sons incorporated.

Cebekhulu, N.P. 2016. *Assessing security measures at hotels*: A case study from Gauteng. Unpublished dissertation, MA Criminal Justice. Pretoria: University of South Africa.

Cherry, K .2018. *Sample types and sampling errors in research.* Available at https:// www.verywellmind.com/ what –is-a-sample-2795877(accessed on:16 March 2022.

Clutton, A.2018. *The evolution of access control systems*. November:2

Cohen, L.E. & Felson, M. 1980. *Human ecology and crime*: A routine activity approach*.* Human ecology, 8(4), 398-404.

Cooppernica, N. 2020 *Physical and environmental*. CISSP All in One Exam Guide, Elsevier. Amsterdam- Boston. Heidelberg-London.

Cooppernica, N. 2020 *Access control domain.* CISSP All in One Exam Guide, Elsevier. Amsterdam-Boston. Heidelberg-London.

Conrad, E.; Misenar, S. & Feldman, J. 2012. *CISSP study guide*, 2nd edition, Elsevier. Amsterdam-Boston. Heidelberg-London.

Creswell, J.W. & Creswell, J.D. 2016. *Research design*: *Qualitative, quantitative, and mixed methods approaches*. Fourth edition. Thousand Oaks, Calif: Sage.

Creswell, J.W. & Creswell, J.D. 2018. *Research design*: *Qualitative, quantitative, and mixed methods approaches*. Fifth edition. Thousand Oaks, Calif: Sage.

Denscombe, M. 2002. *Ground rules for good research*: *A 10-point guide for social researchers.* Philadelphia. Open University Press.

Department of Public Works. 2013. *Integrated security policy*. Limpopo Provincial Government. Republic of South Africa.

De Vos, A.S Strydom, H. Fouche, C.B. & Delport, C.S.L, 2005 *Research at Grassroots for the Social Sciences and Human Service Professions*, 3rd ed. Pretoria: Van Schaik.

The Editor. 2015. *Mangaung cleans up its books*: The Weekly. 30 January :1.

The Editor. 2017. *Bloemfontein city hall razed during municipal worker dispute*: Times Live. 22 June: 1.

Ekran Security, 2020. *Mandatory access control vs discretionary access control*: Which one to choose? March:11.

Erbschloc, 2017. *Walling out insiders*. *Controlling access to improve organizational security*. CRC Press. Taylor & Francis Group, Boca Raton, London New York.

Esfandi, A & Sabbari, M. 2014. *A security framework for access control in web services*. Department of Computer Engineering Islamic Azad University Borujerd Branch, Iran.

Fay, J. 2011. *Contemporary security management*: Burlington, MA: Butterworth-Heinemann.

Felson, R.B. 1997*.* 'Routine activities and involvement in violence as actor, witness, or target'. *Violence and Victims*, 12(3),209-221.

Fennelly, L.J. 2012. *Effective physical security*.4th ed. Butterworth- Heinemann.

Fernandez, E.B., Ballesteros, J, Desouza-Doucet, A.C. & M.M. Larrondo-Petrie. 2007. *Security patterns for physical access control systems*. Department of

Computer Science and Engineering, Florida Atlanta University. Boca Raton. Florida, USA.

Geriecke, M. 2018. *Municipal offices temporarily closed after robbery*: Express.5 July:1.

Govender, D. 2018. *Claw ethics review committee*: Policy Directives. Paper presented at a workshop for M&D. Brooklyn, Pretoria.12 April.

Greaves, A. 2019. *Security at government buildings*. Independent Assurance Report to Parliament. Victoria Government Printer. May:29 Australia.

Griffiths, A.2020. *Conducting research*: Demarcation of the research. October: 18.

Guennouni, S.; Mansouri, A. & Ahaitouf, A. 2019 *Biometric systems and their applications*. Renewable Energy and Smart System Laboratory, Faculty of Science and Technology, Sidi Mohammed Ben Abdellah University, Fez, Morocco.

Harris, S. 2013. *Access control*. In CISSP Exam guide (6th ed). USA: McGraw-Hill.

HID Security Management, 2020. *The 2020 state of physical access control report.*

Holt, B. 2015. *Best practices for planning and managing physical security resource, an interagency security committee guide.*

Homeland Security. 2016. *Access control technologies handbook*. United States of America Department of Homeland Security, Science and Technology Directorate.

Horn, R.E. 2012. *A pro-active approach to curb asset theft at a South African mine*. MTech Unpublished dissertation. Pretoria: University of South Africa.

Houlis, P. 2018. *From keypad to iris recognition. The history and future of access control credentials*. IFSEC GLOBAL, ASSA ABLOY.

Hutter, D. 2016. *Physical security and why it is important? The importance of physical security*. The SANS Institute

Karimi, V.R.; Alencar, P.S.C. & Cowan, D.D. 2016. *A formal modelling and analysis approach for access control rules, policies and their combinations*. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada. Springer-Verslag Berlin Heidelberg.

Kersley, S. 2019*. Biometric: the future is in your hands*. Vol 50 issue 4, p663-669. Loyola of Los Angeles Law Review.

Kole, O.J. 2014. *Industrial security in practice*. Study guide for SEP 2602. Pretoria: University of South Africa.

Korstjens, I. & Moser, A. 2018. *Practical guidance to qualitative research*. *trustworthiness and publishing*, Part 4: European Journal of General Practice, 24:1.120-124 DOI:10.1080/13814788.2017.1375092.

Lekubu, B.K. 2015. *Manifestation of corruption in the city of Tshwane metropolitan municipality*. Un.p.ublished MTech, Security Management. Pretoria. University of South Africa.

Lombard, C. 2013. *Security Principles & Practices*. Study guide for SEP 1501. Pretoria: University of South Africa.

Mahambane, M.A. 2014. *Security technology and information security*. Study guide for SEP 1501. Pretoria: University of South Africa.

Mangaung Metropolitan Municipality. *Integrated Development Plan 2018/19, version 11.*

Mangaung Metropolitan Municipality. *Risk register*, 2017/18.

Mangaung Metropolitan Municipality. *Crime report*, 2018.

McCombe,S. 2019.*Sampling methods/ types and techniques explained*. Scribbr.September: 19.

Maxfield, M.G. & Babbie, E. 1995. *Research methods for criminal justice and criminology*. 2nd edition. Belmont: Wadsworth.

McCrie, R.D. 2007. *Security operations management*. 2nd edition. Amsterdam; Boston: Butterworth- Heinemann/ Elsevier.

Minnaar, A.de V. 2016. *Criminal Justice Research Methodology*. Study guide for SEP 3707. Pretoria: University of South Africa.

Mistry, D., Minnaar, A., Patel, C. & Rustin, C. 2003. *Criminal Justice Research Methodology*. South Africa: Technikon SA.

Moore, J. 2020. *Physical security trends for 2020*. IFSEC GLOBAL.

Moses, B.S. & Rowe, D.C. 2016. *Physical security and cybersecurity: reducing risk by enhancing physical security posture through multi-factor authentication and other techniques*. International Journal for Information Security Research (IJISR), Volume 6, Issue 2, June. Cyber Security Research Lab. Birmingham Young University.

Moyo, S. 2019. *Evaluating the use of CCTV surveillance systems for crime control and prevention*: Selected case studies from Johannesburg and Tshwane Gauteng. Unpublished MTech Dissertation. Pretoria.

Muchengetwa, S. 2019. *Comparative analysis of quantitative and qualitative research designs-long version*. Paper presented at a workshop for M&D. Bloemfontein.26 March.

Mudondo, SM.2021. *Data analysis and methods of qualitative research*: *Emerging research and opportunities*, IGI Global, pp1-31. https:// On-doi-org.oasis.unisa.ac.za/10.4018/978-1-7998.

Mudondo, SM.2021. *Ethics in qualitative research*: Emerging research and opportunities, IGI Global, pp77-98. https: On-doi-org.oasis.unisa.ac.za /10418-1-7998 ch004.

Mudondo, SM.2021. *The trustworthiness in qualitative research output:* Emerging research and opportunities, IGI Global pp 121-139 https: On-doi-org.oasis.unisa.ac.za / 10.4018/978-1-7998-8549-8-ch006.

Mukherjee, S.P. 2020. *A guide to research methodology*. 1st edition, CRC Press, New York.

Munanga, V.N.K & Illaiah, P. 2014. *Research development in biometrics and video processing technique*. Hershley- PA: IGI Global.

Niles, S. 2011*. Physical security in mission critical facilities*. White paper 82. Schneider Electrics.com.

Norman, T.L. 2016. *Risk analysis and security countermeasures selection*. CRC Press. Taylor and Francis Group. Boca Raton, London. New York.

Pieterse, G. 2017 *Access control systems*: A Preparatory study to aid in the development of a minimum technology standard for access control system deployment as part of the overall facility risk management strategy.

Polit, DF& Beck, CT. 2014. *Essentials of nursing research*: Appraising evidence for nursing practice.8th ed.Philadelphia, PA: Wolters Kluver/ Lippincott Williams & Wilkings.

Pretorius, W.L. 2012. *A criminological analysis of copper cable theft in Gauteng*. Unpublished dissertation, MA in Criminology. Pretoria: University of South Africa.

Queiros, A., Faria, D.& Almeida, F.2017. *Strengths and limitations of qualitative and quantitative research methods*. European Journal of Education Studies, 3(9), 369-387.

Rao, U.H. & Nayak, U.2014. *Physical security and biometrics*. The infosec handbook. ISBN. 9781-4302-6382-1.

Rao, UH & Nayak, U.2014*. Physical security and biometric*, In: The infosec handbook, pp. 293-306 Appress, Berkely, CA.

Rath, AT.2015. *Managing and enforcing privacy awareness policies in IT systems.* Unpublished PhD thesis. University of Namur. Belgium.

Reniers, G.; Conzzani, D. & Khakzad, V. 2017. *Safety and reliability*. *Safe Societies in a changing world*. CRC Press. Taylor and Francis Group. Boca Raton, London. New York.

Richey, D. 2019.Tailgating: *A common courtesy and a common risk Security:* Try. vol 56, Issue 9. Pages 52,54-55.

Rhodes, B. 2020. *Vehicle gate access control guide*. IPVM. EDT.

Sabhanayagam, T; Venkatesan& Senthamaraikanna .2018. *A comprehensive survey on various biometric systems*. Centre for Computer and Information Technology Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India.

Sandhu, R.S. 1993. *Lattice-based access control models*. IEEE Computer, 26(11): 9-19.

Saflec Systems. 2018. *The importance and benefits of biometric readers*.12 June (accessed on 23/8/2019.

Saflec Systems. 2018. *How can biometrics secure* a *return on investment?* 17 July (accessed on 23/8/2019).

Saflec Systems. 2018. *The importance and benefits of biometric readers*. 12 June (accessed on 23/8/2019).

Smith, C.L. & Brook, D.L. 2013.*Security science*: *The theory and practice of security*. Waltham, MA: Butterworth-Heinemann.

Smith, M. & Mann, M. 2018*. Biometrics, Crime and Security*. Ist edition, Routledge. London.

Smith, R.G.; Gannoni, A. & Goldsmid, S. 2019. *Use and acceptance of biometric technologies in 2017*. *Trends & Issues in Crime &Criminal Justice*. Issue 569, pp1-18.18p.2 Charts, 5 Graphs. Australian Institute of Criminology.

South African Government. 1985. *Control of Access to Public Premises and Vehicle Act* 53 of 1985.*Trespass Act 6* of 1985. Pretoria: Government Printer.

South African Government. 1996. *The Constitution of the Republic of South Africa*, *Act* 108 of 1996. Pretoria: Government Printer.

South Africa.1998 *Minimum Information Security Standards*.2nd edition., March 1998. Available at http://right2info.org/resources/publications/laws-1/SAMinimum%20Information%20Security%standards.pdf (accessed on12/818)

South African Government. 1998. *Local Government Municipal Structures Act*, No117 of 1998. Pretoria: Government Printer.

South African Government. 1969. *Trespass Act 6 of 1969*. Pretoria: Government Printer.

Speed, T.S. 2016. *Asset protection through security awareness*. CRC Press. Taylor and Francis Group. Boca Raton. London. New York.

Statistics South Africa, *Community survey* 2016.

Statistics solutions. 2020. *What is trustworthiness in qualitative research?*

Swart, B. 2020. *Interview conducted on an overview of access control measures in the Mangaung Metropolitan municipality regional offices*.

Tabane, R. 2019.*Literature review research. Review of scholarship*. Paper presented at a workshop for M&D. Bloemfontein.26 March.

Taole, M.J. 2019. *Qualitative data analysis.* Paper presented at a workshop for M & D. Bloemfontein.26 March.

Thoka, E.M. 2021. An *evaluation of security threats and vulnerabilities to a national key point: Case study of medupi power station.* Un.p.ublished dissertation, M tech in Security Management. Pretoria: University of South Africa.

Tlape, O.P.L. 2019. *Investigating the effectiveness of the access control system at Sol Plaatjie University, in Kimberley, Northern Cape Province*. MBA Un.p.ublished mini dissertation, Mahikeng: North West University.

Truet, A.; Rickes B.E. & Dingle J. 2015. *Physical security and safety*. *A field guide for the practitioner.* CRC Press. Taylor &Francis Group, Boca Raton, London New York.

Umbrella Technologies. 2019. *Access control systems and its effectiveness.*

Van Biljon, W.R. 2013. *Role-based access control using dynamically shared cloud accounts*, IFI CLAIMS. Patent Services. Symantec Corporation, California. USA.

Van Jaarsveld, L. 2011. *An investigation of safety and security measures at secondary schools in Tshwane*, *South Africa*. Un.p.ublished dissertation, MTech Security management. Pretoria: University of South Africa.

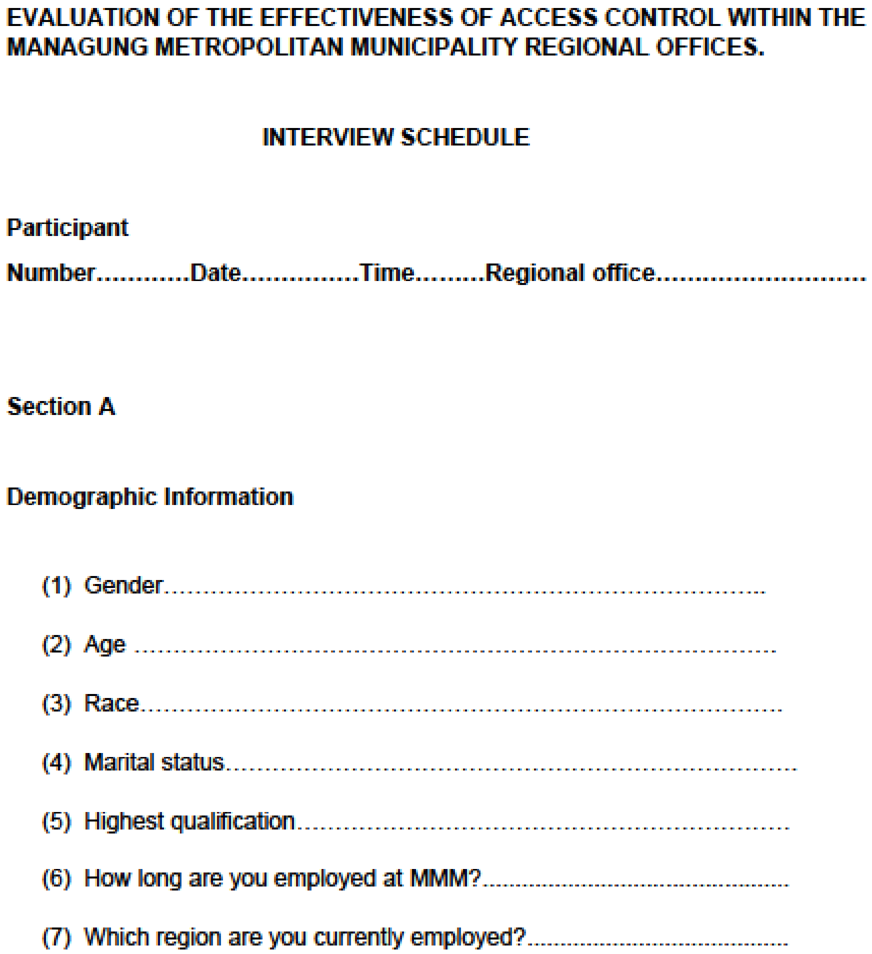
Walliman, N. 2011. *Research Methods*, *the basics*. USA: Routledge.

Yaokumah, W. 2018. *Inter-organizational study of access control security measures*. International Journal. Pf Technology and Human Interaction, 14(1): 60-79. DOI 10.4018/ IJTHI.2018010104. University of Ghana.

Zhang,Y .& Wildemuth, BM. 2016. *Theme development in qualitative content analysis and thematic analysis.* Westport: Libraries unlimited.

ANNEXURES

ANNEXURE A: INTERVIEW SCHEDULE



EVALUATION OF THE EFFECTIVENESS OF ACCESS CONTROL WITHIN THE MANAGUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICES.

INTERVIEW SCHEDULE

Participant

Number…………Date……………Time………Regional office………………………..

Section A

Demographic Information

(1) Gender…………………………………………………………………..

(2) Age ……………………………………………………………………………

(3) Race……………………………………………………………………………

(4) Marital status……………………………………………………………………

(5) Highest qualification…………………………………………………………

(6) How long are you employed at MMM?..

(7) Which region are you currently employed?...

Section B

This section deals with an overview of various aspects of access control at Mangaung metropolitan municipality

1. What existing access control measures are in place in your regional office?

2. How effective are these measures to protect property, assets, employees, contractors and members of the public?

3. What are the weaknesses of access control in your regional office?

4. How access control is operated for both visitors and employees in your regional office?

5. Who are the key players in the implementation of access control in your regional office?

Section C

This section deals with security risks and vulnerabilities confronting the Mangaung metropolitan municipality regional offices at access control points.

1. What are the important assets that need protection at access control points in the regional office?

2. What security risks are at access control points in your regional office?

3. How vulnerable are employees, visitors and contractor in the premises of the regional office?

4. What security breaches relating to access control normally occur in the regional office?

5. Who are the perpetrators of these breaches relating to access control in your regional office?

Section D

This section deals with recommended access control measures to be implemented in the regional offices.

1. Which security measures must your regional office implement to manage access control?

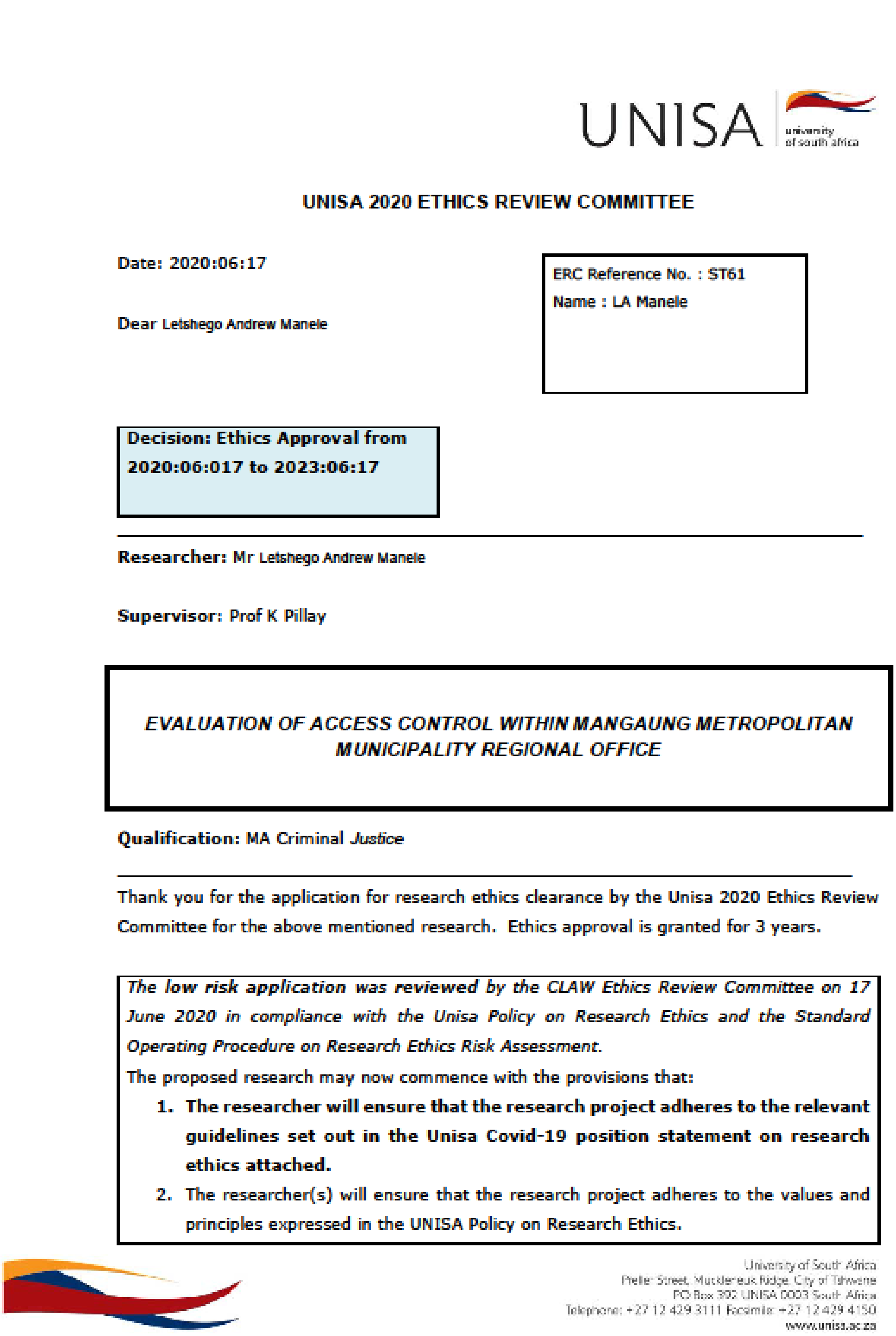
2. What access control measures should be implemented to monitor and detect unauthorized entry of people into the premises of the regional office?

3. How should access control be improved in the future to ensure the safety of property, assets, employees and visitors in the regional office?

4. Where should access control for employees, visitors and contractors be regulated in your regional office?

5. Why should access control be integrated with other security measures?

ANNEXURE B: UNISA ETHICAL CLEARANCE LETTER



UNISA university of south africa

UNISA 2020 ETHICS REVIEW COMMITTEE

Date: 2020:06:17

ERC Reference No. : ST61
Name : LA Manele

Dear Letshego Andrew Manele

Decision: Ethics Approval from 2020:06:017 to 2023:06:17

Researcher: Mr Letshego Andrew Manele

Supervisor: Prof K Pillay

EVALUATION OF ACCESS CONTROL WITHIN MANGAUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICE

Qualification: MA Criminal *Justice*

Thank you for the application for research ethics clearance by the Unisa 2020 Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

The ***low risk application*** *was* ***reviewed*** *by the CLAW Ethics Review Committee on 17 June 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. **The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.**
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date **2023:06:17**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

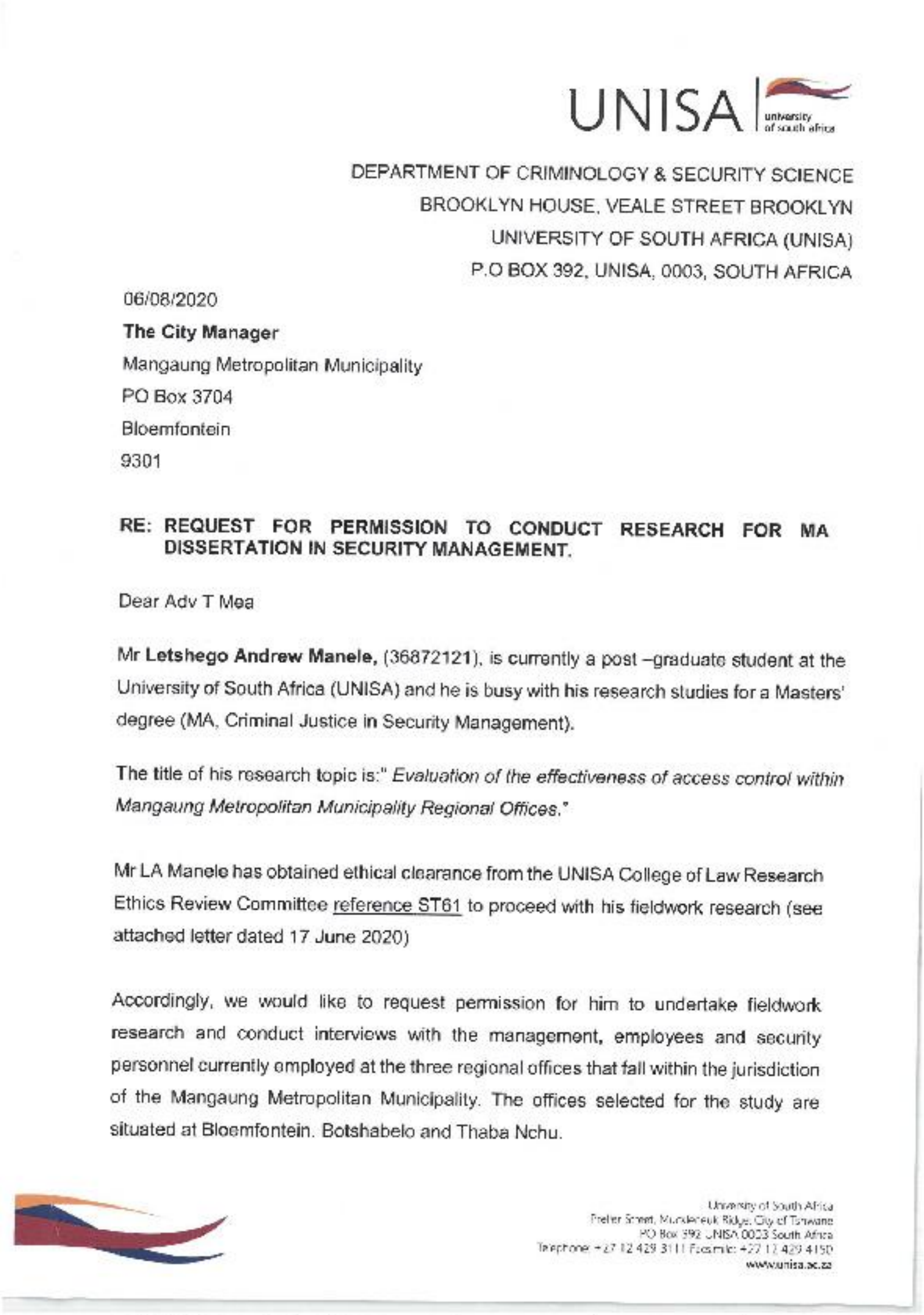
The reference number ST 61-2020 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

Prof T Budhram
Chair of CLAW ERC
E-mail: budhrt@unisa.ac.za
Tel: (012) 433-9462

Prof M Basdeo
Executive Dean : CLAW
E-mail: MBasdeo@unisa.ac.za
Tel: (012) 429-8603

ANNEXURE C: LETTER OF PERMISSION TO CONDUCT RESEARCH



DEPARTMENT OF CRIMINOLOGY & SECURITY SCIENCE
BROOKLYN HOUSE, VEALE STREET BROOKLYN
UNIVERSITY OF SOUTH AFRICA (UNISA)
P.O BOX 392, UNISA, 0003, SOUTH AFRICA

06/08/2020

The City Manager
Mangaung Metropolitan Municipality
PO Box 3704
Bloemfontein
9301

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH FOR MA DISSERTATION IN SECURITY MANAGEMENT.

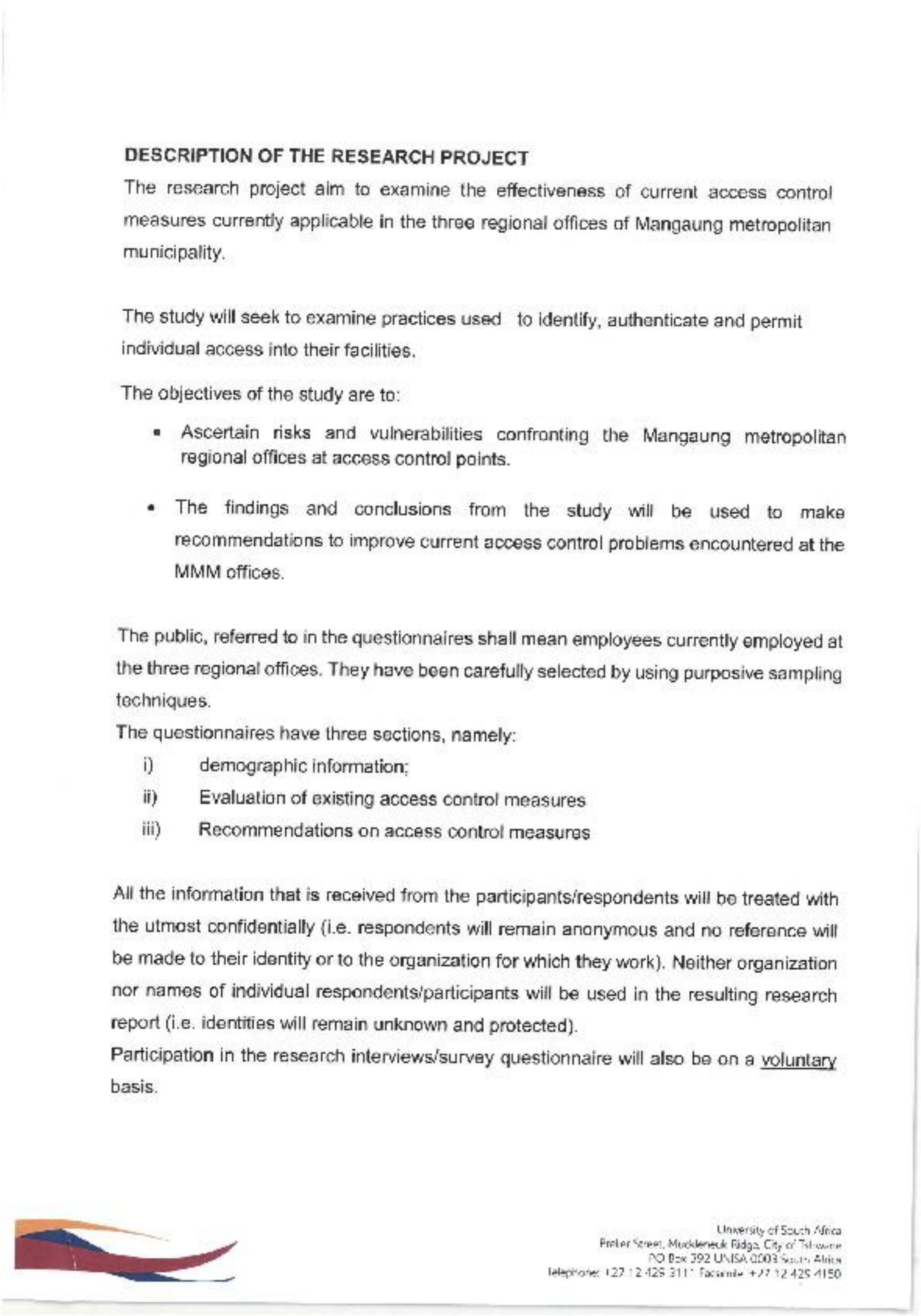
Dear Adv T Mea

Mr **Letshego Andrew Manele,** (36872121), is currently a post –graduate student at the University of South Africa (UNISA) and he is busy with his research studies for a Masters' degree (MA, Criminal Justice in Security Management).

The title of his research topic is:" *Evaluation of the effectiveness of access control within Mangaung Metropolitan Municipality Regional Offices.*"

Mr LA Manele has obtained ethical clearance from the UNISA College of Law Research Ethics Review Committee reference ST61 to proceed with his fieldwork research (see attached letter dated 17 June 2020)

Accordingly, we would like to request permission for him to undertake fieldwork research and conduct interviews with the management, employees and security personnel currently employed at the three regional offices that fall within the jurisdiction of the Mangaung Metropolitan Municipality. The offices selected for the study are situated at Bloemfontein, Botshabelo and Thaba Nchu.



DESCRIPTION OF THE RESEARCH PROJECT

The research project aim to examine the effectiveness of current access control measures currently applicable in the three regional offices of Mangaung metropolitan municipality.

The study will seek to examine practices used to identify, authenticate and permit individual access into their facilities.

The objectives of the study are to:

- Ascertain risks and vulnerabilities confronting the Mangaung metropolitan regional offices at access control points.
- The findings and conclusions from the study will be used to make recommendations to improve current access control problems encountered at the MMM offices.

The public, referred to in the questionnaires shall mean employees currently employed at the three regional offices. They have been carefully selected by using purposive sampling techniques.

The questionnaires have three sections, namely:

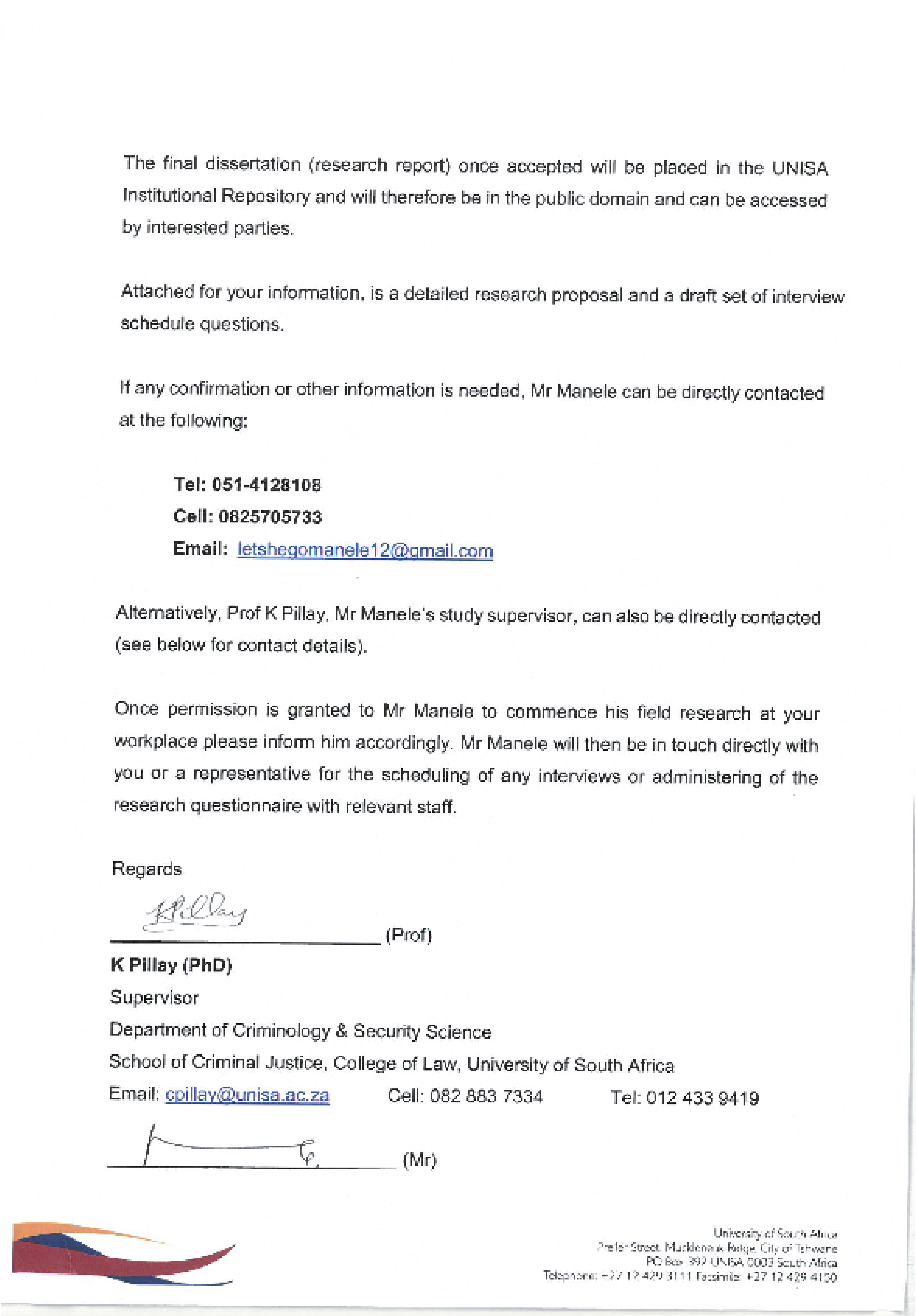
i) demographic information;

ii) Evaluation of existing access control measures

iii) Recommendations on access control measures

All the information that is received from the participants/respondents will be treated with the utmost confidentially (i.e. respondents will remain anonymous and no reference will be made to their identity or to the organization for which they work). Neither organization nor names of individual respondents/participants will be used in the resulting research report (i.e. identities will remain unknown and protected).

Participation in the research interviews/survey questionnaire will also be on a voluntary basis.



The final dissertation (research report) once accepted will be placed in the UNISA Institutional Repository and will therefore be in the public domain and can be accessed by interested parties.

Attached for your information, is a detailed research proposal and a draft set of interview schedule questions.

If any confirmation or other information is needed, Mr Manele can be directly contacted at the following:

Tel: 051-4128108
Cell: 0825705733
Email: letshegomanele12@gmail.com

Alternatively, Prof K Pillay, Mr Manele's study supervisor, can also be directly contacted (see below for contact details).

Once permission is granted to Mr Manele to commence his field research at your workplace please inform him accordingly. Mr Manele will then be in touch directly with you or a representative for the scheduling of any interviews or administering of the research questionnaire with relevant staff.

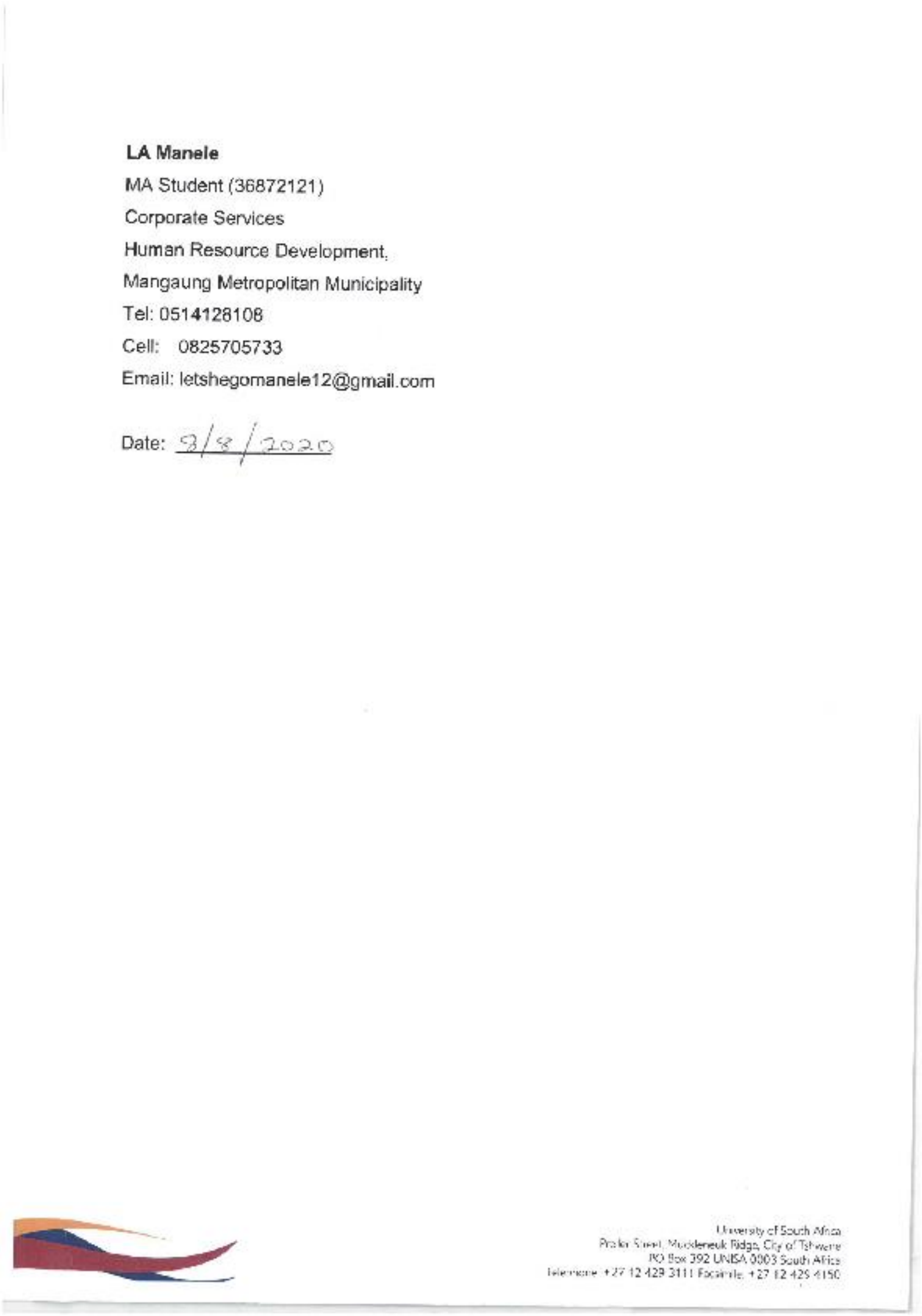
Regards

KPillay

______________________ (Prof)

K Pillay (PhD)
Supervisor
Department of Criminology & Security Science
School of Criminal Justice, College of Law, University of South Africa
Email: cpillay@unisa.ac.za Cell: 082 883 7334 Tel: 012 433 9419

______________________ (Mr)



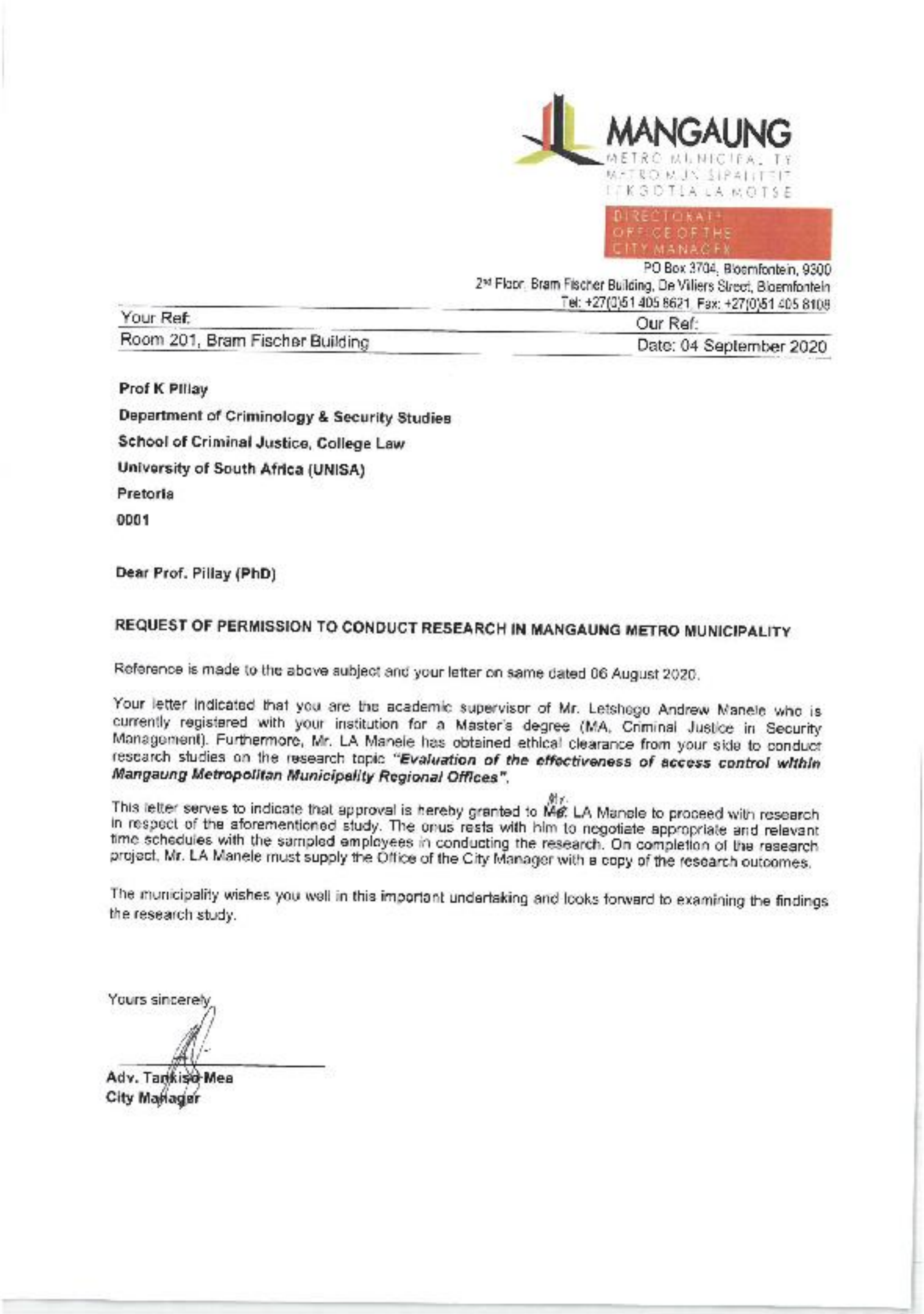
LA Manele

MA Student (36872121)
Corporate Services
Human Resource Development,
Mangaung Metropolitan Municipality
Tel: 0514128108
Cell: 0825705733
Email: letshegomanele12@gmail.com

Date: 8/8/2020

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150

ANNEXURE D: RESEARCH PERMISSION LETTER



MANGAUNG
METRO MUNICIPALITY
METRO MUNISIPALITEIT
LEKGOTLA LA MOTSE

DIRECTORATE
OFFICE OF THE
CITY MANAGER

PO Box 3704, Bloemfontein, 9300
2nd Floor, Bram Fischer Building, De Villiers Street, Bloemfontein
Tel: +27(0)51 405 8621 Fax: +27(0)51 405 8108

Your Ref:
Room 201, Bram Fischer Building

Our Ref:
Date: 04 September 2020

Prof K Pillay
Department of Criminology & Security Studies
School of Criminal Justice, College Law
University of South Africa (UNISA)
Pretoria
0001

Dear Prof. Pillay (PhD)

REQUEST OF PERMISSION TO CONDUCT RESEARCH IN MANGAUNG METRO MUNICIPALITY

Reference is made to the above subject and your letter on same dated 06 August 2020.

Your letter indicated that you are the academic supervisor of Mr. Letshego Andrew Manele who is currently registered with your institution for a Master's degree (MA, Criminal Justice in Security Management). Furthermore, Mr. LA Manele has obtained ethical clearance from your side to conduct research studies on the research topic ***"Evaluation of the effectiveness of access control within Mangaung Metropolitan Municipality Regional Offices"***.

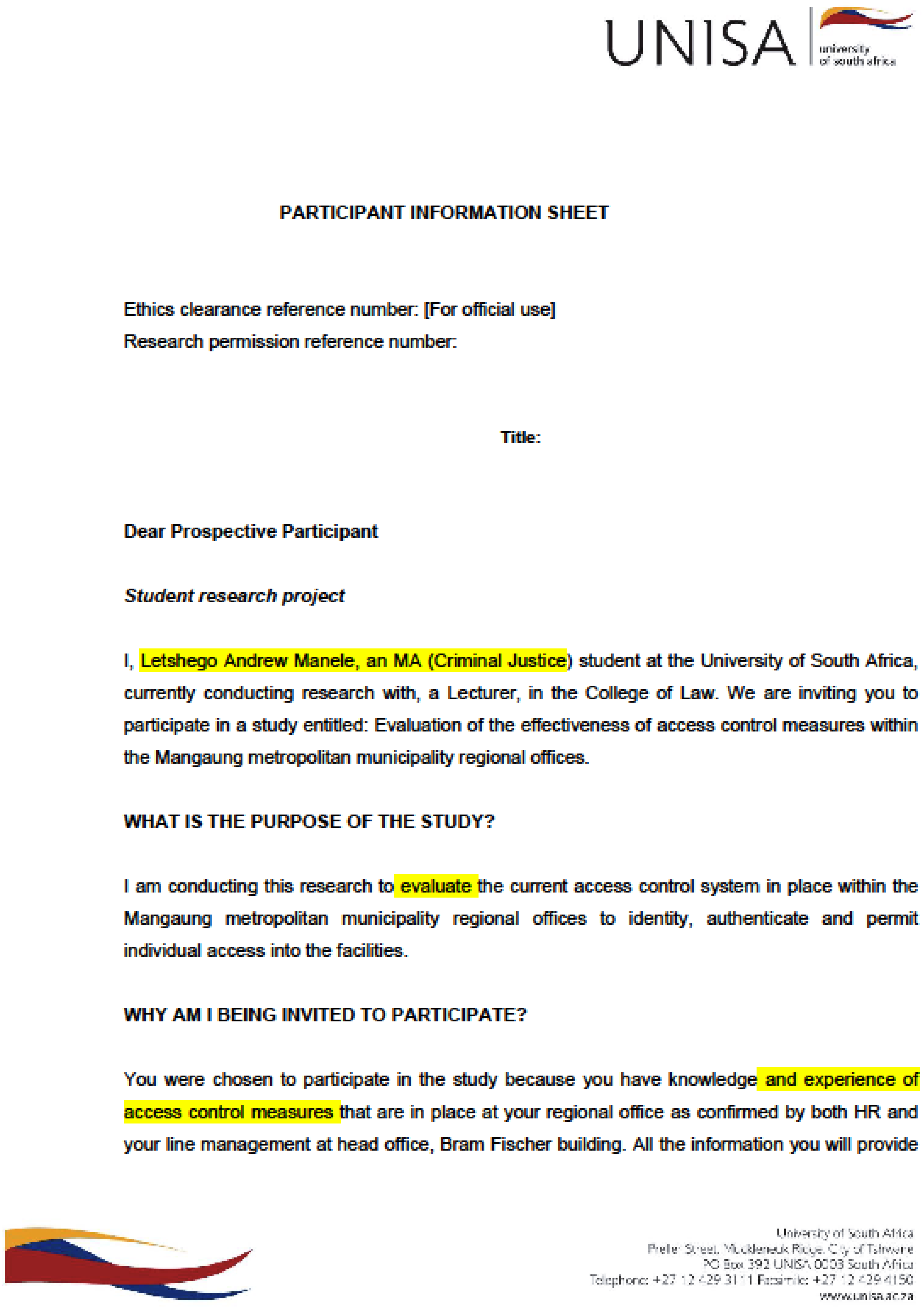
This letter serves to indicate that approval is hereby granted to ~~Ms~~ Mr. LA Manele to proceed with research in respect of the aforementioned study. The onus rests with him to negotiate appropriate and relevant time schedules with the sampled employees in conducting the research. On completion of the research project, Mr. LA Manele must supply the Office of the City Manager with a copy of the research outcomes.

The municipality wishes you well in this important undertaking and looks forward to examining the findings the research study.

Yours sincerely

Adv. Tankiso Mea
City Manager

ANNEXURE E: PARTICIPANT INFORMATION SHEET



PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: [For official use]
Research permission reference number:

Title:

Dear Prospective Participant

Student research project

I, Letshego Andrew Manele, an MA (Criminal Justice) student at the University of South Africa, currently conducting research with, a Lecturer, in the College of Law. We are inviting you to participate in a study entitled: Evaluation of the effectiveness of access control measures within the Mangaung metropolitan municipality regional offices.

WHAT IS THE PURPOSE OF THE STUDY?

I am conducting this research to evaluate the current access control system in place within the Mangaung metropolitan municipality regional offices to identity, authenticate and permit individual access into the facilities.

WHY AM I BEING INVITED TO PARTICIPATE?

You were chosen to participate in the study because you have knowledge and experience of access control measures that are in place at your regional office as confirmed by both HR and your line management at head office, Bram Fischer building. All the information you will provide

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

will be treated as confidential and nowhere in the study will your name be mentioned, and all the information provided by you will solely be used for the purpose of this research study.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves interviews and the participants is expected to answer the questions asked as honest as possible. The participants will be expected to answer in-depth questions and the duration for the interviews will be between 30- 60 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Statement that participation is voluntary and that there is no penalty or loss of benefit for non-participation. Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

The participants won't benefit any money or there won't be any financial gain. But the participants will benefit because the information they have provided will assist the regional offices in their operations, methods and strategies.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

There won't be any negative consequences for the participants who will participate in the study

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

You have the right to insist that your name will not be recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about your involvement in this research which will adhere to the principle of confidentiality . Your details will remain anonymous which will not be recorded anywhere and no one will be able to connect you to the answers you give . Your answers will be given a code number, or a pseudonym and you will be referred to confidentially in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder, and members of the Research Ethics Review Committee.

Only the researcher will have access to the data and the confidentiality will be maintained in line with the university ethics code for researchers. However, you need to realize that your information can be used in the researcher articles or conference proceedings, it is not only for the purpose of this study. Otherwise, records that identify you will be available only to people working on the study, unless you give permission for other people to see the records.

.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a period of five years in a locked cupboard/filing cabinet in the office of the researcher for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Indicate how information will be destroyed if necessary.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

No payment or any incentives for participating in this study will be provided by the researcher to participants.

HAS THE STUDY RECEIVED ETHICS APPROVAL

This study has received written approval from the Research Ethics Review Committee of the Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

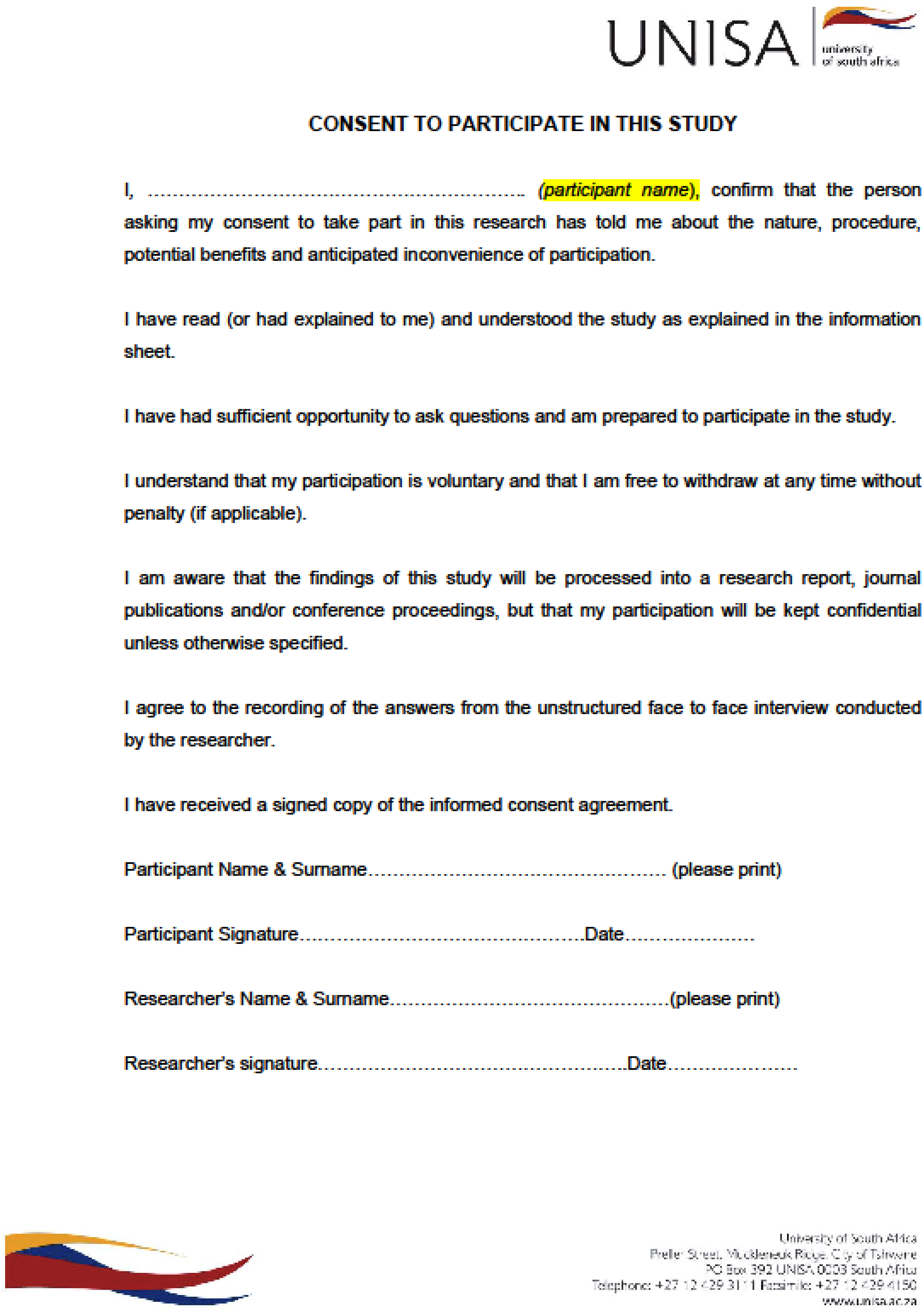
If you would like to be informed of the final research findings, please contact Letshego Andrew Manele at 0825705733 or email address: letshegomanele12gmail.com, the findings are accessible for 2022.

Should you have concerns about the way in which the research has been conducted, you may contact 0828837334email: cpillay@unisa.ac.za

Thank you for taking time to read this information sheet and for participating in this study.

Thank you.

ANNEXURE F: PARTICIPANT CONSENT FORM



UNISA university of south africa

CONSENT TO PARTICIPATE IN THIS STUDY

I, ………………………………………………………. *(participant name)*, confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the answers from the unstructured face to face interview conducted by the researcher.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname………………………………………… (please print)

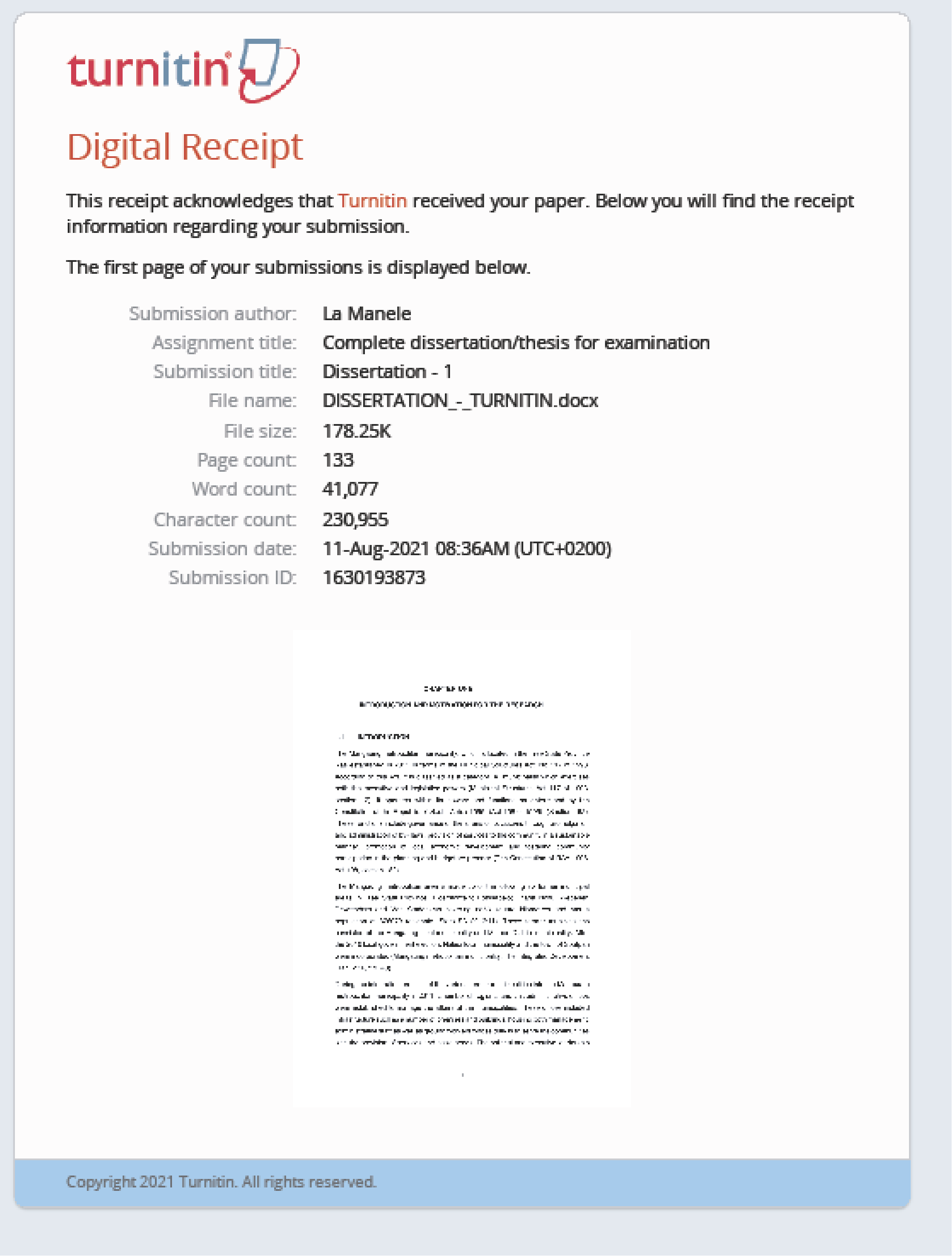
Participant Signature…………………………………………Date…………………

Researcher's Name & Surname………………………………………(please print)

Researcher's signature…………………………………………..Date…………………

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE G: TURN IT IN REPORT



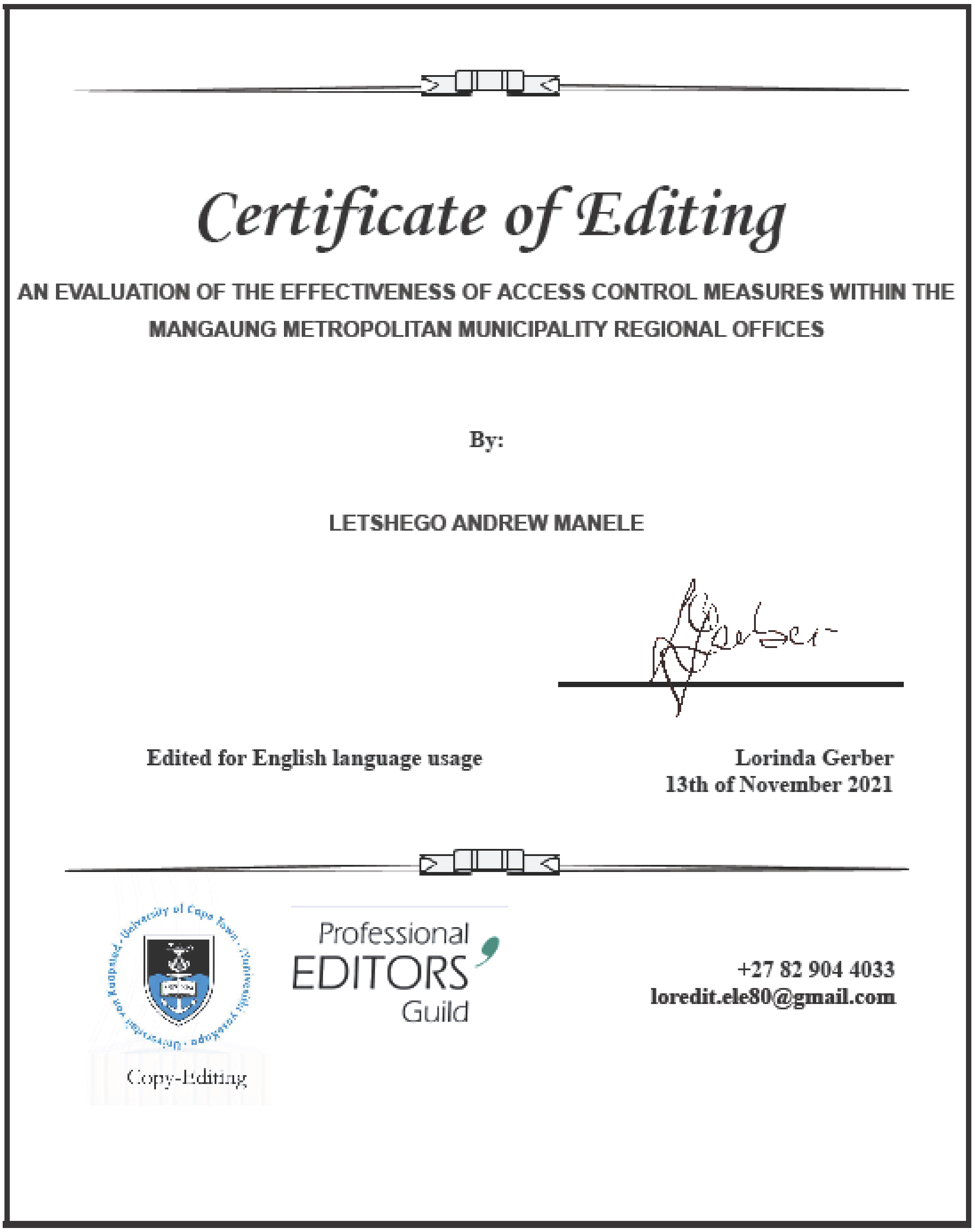
Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	La Manele
Assignment title:	Complete dissertation/thesis for examination
Submission title:	Dissertation - 1
File name:	DISSERTATION_-_TURNITIN.docx
File size:	178.25K
Page count:	133
Word count:	41,077
Character count:	230,955
Submission date:	11-Aug-2021 08:36AM (UTC+0200)
Submission ID:	1630193873

ANNEXURE H: EDITING CERTIFICATE



Certificate of Editing

AN EVALUATION OF THE EFFECTIVENESS OF ACCESS CONTROL MEASURES WITHIN THE MANGAUNG METROPOLITAN MUNICIPALITY REGIONAL OFFICES

By:

LETSHEGO ANDREW MANELE

Edited for English language usage

Lorinda Gerber
13th of November 2021

Copy-Editing

Professional EDITORS Guild

+27 82 904 4033
loredit.ele80@gmail.com