ESWATINI NATIONAL CYBERSECURITY STRATEGY 2020 - 2025

(SZ NCS 2025)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Kingdom of Eswatini, like all other nations worldwide, is facing fundamental changes resulting from on-going digitalisation. Indeed, as Information and Communication Technologies (ICTs) continue to evolve rapidly, and are increasingly integrated in national and global economies, and so is the increasing dependency on ICTs in the way individuals, institutions and nations function. The Kingdom of Eswatini is fully cognisant of the fact that the extensive integration of ICTs in its society, especially within its public sector, is essential to its on-going efforts to develop the prosperity and welfare of its citizens and the country in general. That is why the Kingdom of Eswatini is actively undertaking several initiatives to promote the adoption and usage of ICTs in all facets of its society and economy. Examples of these initiatives include the on-going implementation of the National E-Government Strategy. The on-going development of a National Broadband Strategy for Eswatini, and the review of its National Information and Infrastructure and Communication Policy (Implementation Plan 2012 - 2016) just to mention a few.

As Eswatini embarks on transforming its economy and society by integrating ICTs across its economy and society, it is imperative that it takes into account the effects of such a transformation, which include among others, the need for security and integrity of data, systems, networks, digital infrastructure and cyberspace by businesses, public institutions, individuals, critical service providers, etc.

This National Cybersecurity Strategy of Eswatini 2020 - 2025 (SZ NCS 2025) describes a coherent national approach for protecting Eswatini's data, systems and networks from cyber threats. This strategy will provide guidance to all relevant stakeholders on their specific roles and responsibilities for cybersecurity by setting the national Vision and Strategic Objectives with respect to cybersecurity in Eswatini.

This strategy outlines essential elements necessary for ensuring a good cybersecurity posture of Eswatini and these include:

- The current context of cybersecurity of Eswatini including current and emerging cyber threats relevant to Eswatini
- Eswatini's national cybersecurity vision and the Strategic Goals that will support the attainment of that vision
- Principles that will underpin the implementation of this strategy
- Roles and responsibilities of identified relevant stakeholders
- The manner in which this strategy will be implemented

- How progress in implementing this strategy and achieving its objectives would be evaluated.

- The Kingdom of Eswatini's Vision for Cybersecurity is:

"A safe, secure and resilient Cyberspace in Eswatini"

The Kingdom of Eswatini will embark on achieving the following 5 Strategic Goals to attain its National Vision:

- ***Strategic Goal 1****: Enhance the security and resilience of national critical information infrastructure and other related ICT systems*

- ***Strategic Goal 2****: Strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini*

- ***Strategic Goal 3****: Build Eswatini's capacity and expertise in cybersecurity*

- ***Strategic Goal 4****: Foster a safe and secure information society for Eswatini*

- ***Strategic Goal 5****: Strengthen cooperation, collaboration and partnerships on cybersecurity*

This strategy provides the right framework for the Kingdom of Eswatini to effectively integrate secure ICTs across all segments of its society and economy. This will transform and enhance Eswatini's future wellness and prosperity.

1 INTRODUCTION

As the Kingdom of Eswatini embarks on transforming its economy and society by integrating ICTs across its economy and society, it is imperative that it takes into account the effects of such a transformation which includes among others, the need for security and integrity of data, systems, networks, digital infrastructure and cyberspace by businesses, public institutions, individuals, critical service providers, etc. Indeed, with national and global trends and events demonstrating that all nations, including the Kingdom of Eswatini, continue to face increasingly sophisticated malicious cyber threat actors as well as a constantly evolving cyber threat landscape, it is crucial that The Kingdom of Eswatini takes effective measures to ensure Eswatini's cyberspace is secure.

This strategy describes the approach of the Kingdom of Eswatini in responding to both current and emerging cyber threats, and how the Kingdom of Eswatini intends to defend its interests in cyberspace. This strategy considers and builds on several national priorities of Eswatini, which are defined in a number of relevant policies, legal and regulatory instruments for Eswatini. In addition, the strategy goes further and describes a comprehensive approach for protecting Eswatini's data, information systems and networks, which is based on a multi-stakeholder approach in ensuring this objective is achieved. The success of such an approach requires continuous resource investment by all stakeholders in enhancing their capabilities and skills base in protecting their systems and data from current cyber threats, and outpacing the continuously evolving and emerging cyber threats.

1.1 Scope of Strategy

This strategy describes a coherent and national approach for protecting Eswatini's data, information systems and network infrastructure from cyber threats. This strategy provides guidelines to all relevant stakeholders on their expected roles and responsibilities in achieving the national Vision and Strategic Objectives of the National Cybersecurity Strategy for Eswatini.

This strategy also targets all sectors of the country's economy and society including individuals, private and public sector organisations, academia, civil society organisations, etc. and sets out recommended actions to be undertaken across key focus areas identified stakeholders in the Kingdom of Eswatini. This strategy will also underpin all international engagements undertaken by the Kingdom within the context of ensuring a safe and secure cyberspace.

The successful implementation of this strategy by the Kingdom of Eswatini, will go a long way to support the full attainment of the benefits of digitisation of Eswatini, and supports the prosperity and wellness of all its citizens.

In order to clearly outline the cybersecurity posture of Eswatini, the following core elements will be considered: -

- The current status of cybersecurity in Eswatini, including both current and emerging cyber threats facing the country;
- The national cybersecurity strategy vision and the strategic goals, which will support the achievement of the vision;
- Principles that will underpin the implementation of this Strategy;
- Roles and responsibilities of relevant stakeholders;
- The implementation and monitoring of this strategy.

1.2 Strategy Context

The Kingdom of Eswatini is currently experiencing significant changes in its ICT sector. This is evident with the establishment of an independent telecommunications regulator— Eswatini Communications Commission (ESCCOM) in 2013; the on-going liberalisation of the sector with the issuance of a licence to a third national mobile operator in 2016; and the pending unbundling of EPTC's telecommunications infrastructure and services as an operator. These efforts have started to have an impact on the ICT sector for Eswatini, resulting in improvements in the access and quality of ICT services through 3G and 4G mobile broadband services, which were recently introduced in Eswatini.

With a population of about 1.15 million people, a mobile penetration rate of over 98%, with nearly 849,121 mobile broadband users and about 24,572 fixed broadband users; the scale of ICT adoption and the resulting impacts are increasingly noticeable across the Kingdom of Eswatini. This is a key motivation for the Kingdom of Eswatini to continue to leverage its legal and regulatory framework to promote the growth of ICTs and digitisation of its society and economy in a secure environment. The current global trends show that the increasing digitisation of Eswatini will result in increased dependency of Eswatini's economy and society on ICT. Increased dependency on ICT also in turn provides opportunities for cyber threat actors to attempt to attack or illegally access and damage data, information systems and networks in Eswatini. Given that the Cyberspace is borderless, criminals continue to increase their capacities and activities to attack countries across the world, including Eswatini.

In the following sub-section, the strategy provides an overview of some of the known vulnerabilities and threats facing Eswatini today.

1.2.1 Threats

1.2.1.1 Cybercriminals

Cybercrime continues to be a pervasive threat to nations across the world, including Eswatini. Cybercriminals continue to target economic prosperity of individuals, institutions and nations,

since majority of these cybercrimes are financially motivated and incur minimal risk of being caught or identified. There exist two types of cybercrimes namely crimes that can only be executed through the use of ICT devices where the devices are both the target of the crime and the tool for executing the crime (cyber dependent crimes); and traditional crimes whose reach and scale and expanded by the use of ICTs such as computers, computer networks (cyber enabled crimes). An example of cyber dependent crimes includes the deployment of ransomware for launching a specific attack (such as financial gain), whilst an example of cyber enabled crimes include cyber enabled fraud using computers.

Similar to other nations across the world, cybercriminals that commit cybercrimes within Eswatini's jurisdiction might either be based in Eswatini itself, or across the Southern African Development Community (SADC) region, or another part of the world. The Royal Eswatini Police Service has in recent years, been reporting and detecting cybercrime activities, including identifying the perpetrators. However, like other law enforcement forces across the world, the Royal Eswatini Police Service continues to face difficulties in conducting investigations, collecting electronic evidence and prosecuting cybercrimes. These challenges are exacerbated by the sophistication of the cyber-attacks and cross-border nature of the crimes committed. Today, cyber criminals continue to use increasingly sophisticated techniques to commit cybercrimes, and prefer jurisdictions where there is limited investigation and/or reciprocate prosecutorial capabilities.

The Royal Eswatini Police Service is currently enhancing its capacity to investigate cybercrimes, and collaboration with other law enforcement agencies from the SADC region and Interpol to pursue and prosecute cyber criminals. Eswatini will continue to face cyber threats perpetuated by cybercriminals in the foreseeable future. The Wannacry ransomware attack of May 2017 was a global cyber-attack launched by cyber criminals which targeted computers running the Microsoft Windows operating system by encrypting data on these systems and demanding ransom payments in Bitcoin crypto currency. That is an example of the sort of attack cybercriminals are capable of executing, and demonstrates how cybercriminals are employing sophisticated techniques like ransomware and threats of distributed denial of service (DDoS) for extortion. In addition to these threats from organised cybercrime gangs, there are on-going threats resulting from common and less sophisticated cybercrimes, which target small organisations or individuals. These cybercrimes are consistent with global trends of increasing numbers of cyber criminals targeting individuals and businesses for financial pay-outs. These include crimes such as ATM fraud, identity theft, etc.

Eswatini has drafted the Computer and Cyber Crime Bill, which addresses substantive and procedural provisions on cybercrime, and is awaiting enactment by Parliament before coming into law. Apart from this Bill, no legislation currently exists which specifically addresses cybercrime in Eswatini.

1.2.1.2 Hactivism

Hactivism threat actors or hactivist groups tend to attack their targets to promote a political or social agenda. Their motivations are usually either politically or socially motivated. Hacktivist attacks are disruptive in nature and consist of DDoS and website defacements though a few hactivist attacks have inflicted great and sometimes lasting damage to their targets. Eswatini has experienced a number of hactivist related website defacements or DDoS attacks in the past years.

1.2.1.3 Insiders

Organisations across the world including those in Eswatini continue to grapple with the cyber threat posed by insiders commonly called insider threat. Employees with access to critical systems and data belonging to their organisations pose a significant threat to these same organisations. They damage the reputation and to a certain extend the financial position of these organisations deliberately. For instance they could leverage their knowledge to launch or facilitate an attack to disrupt critical functions of their organisation, or steal sensitive data from their organisations. Other than these deliberate acts, insiders could also unintentionally cause harm to their organisations. This could be by downloading unsafe content to company computers, clicking on phishing emails, plugging infected USBs to a computer, etc. These insiders could also be targeted by social engineering techniques of cyber criminals and inadvertently execute actions that negatively impact their organisations and benefit cyber criminals.

1.2.1.4 Cyber Terrorism

Eswatini is fully aware of global trends on cyber terrorism, which includes the use of Internet and especially social networks to radicalise individuals and recruit members into these terrorist groups. These recruits form terrorist cells that eventually execute cyber-attacks against selected target countries.

With the rapid increase in digitisation of developing countries such as Eswatini, there is increasing likelihood that highly technically skilled terrorist groups or lone actors will always emerge with a capability of causing devastating cyber-attacks against target nations. It's therefore imperative that Eswatini prepares adequately for such scenarios by developing a comprehensive National Cybersecurity Strategy that takes such threats into account.

1.2.1.5 States and state-sponsored threats

An emerging threat as observed in the decade is cyber-attacks targeting sovereign nations by either other nations or through state sponsored actors. These nations or state sponsored actors generally seek to unlawfully access either critical information systems, networks or data from targeted states to gain either political, technological, or economic advantages over the targeted nations. Eswatini can potentially become a target of suck an attack, and therefore needs to establish steps to mitigate these threats.

1.2.2 Vulnerabilities

Considering the on-going liberalisation of the ICT sector in Eswatini, and the on-going efforts by Eswatini to increase access and use of ICTs across the nation, it is evident that the Internet will become increasingly integrated in the day-to-day activities of individuals and institutions in Eswatini. Considering the global forecasts[1], which predicts that "Internet of Things" will proliferate rapidly across the world, which implies there will be continuous emergence of vulnerabilities that potentially can be exploited by cyber criminals to cause devastating attacks.

Eswatini needs to put in place measures, good practices and procedures across all segments of its economy and society in order to address the current and emerging vulnerabilities mainly in networks, systems and software. This need cannot be overstated, especially given the recent high profile attack observed worldwide, such as the Wannacry ransomware, which affected services several government and private sector organisations worldwide. Within the context that most successful cyber-attacks result from the successful exploitation of known vulnerabilities that are easily mitigated, the country is obliged to undertake the necessary action to encourage individuals and institutions in Eswatini to invest and take adequate measures to mitigate and manage these vulnerabilities. These measures and the investments need to focus on key areas including technology; individuals and governance.

Another vulnerability threat facing Eswatini relates to the use of unlicensed software and unpatched information systems by either individuals or private/public organisations in Eswatini. Cyber threat actors tend to exploit the vulnerabilities that are inherent in any unlicensed software or unpatched information system. One of the main challenges facing Eswatini today relate to the gaps in skills, knowledge and capabilities required to comprehensively address the cybersecurity needs of the private and public sector of Eswatini. More critical is managing the current risks and threats facing both sectors. A part from IT staff, most senior to board level management of key institutions in Eswatini have a limited understanding of cybersecurity vulnerabilities and threats facing their institutions. It is worth noting that both the Financial Sector and ICT Sector organisations have an understanding for the need for cybersecurity, and have prioritised having cybersecurity awareness programmes and instilling a cybersecurity mindset to staff, especially with respect to good practice in mitigating cyber threats. In general, however, there is no coordinated framework for raising awareness on Cybersecurity across Eswatini. As result the general public in Eswatini tend to have limited and insufficient knowledge and awareness of cybersecurity.

1.3 Cybersecurity Capacity Review

In September 2017, Eswatini with assistance from the International Telecommunication Union (ITU) and Commonwealth Telecommunications Organisation (CTO) conducted a cybersecurity

[1] Roundup Of Internet Of Things Forecasts And Market Estimates, 2016 - https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#368ddbb9292d

capacity review for the country. The review was based on a Cybersecurity Capacity Maturity Model (CMM) developed by CTO's and ITU's implementing partner University of Oxford's Oxford Martin School. The model was used to examine the cybersecurity capacity maturity based on five key dimensions—*Policy & Strategy*; *Culture & Society*; *Education, Training & Skills*; *Legal & Regulatory Frameworks*; and *Standards, Organisations, & Technologies*. Using this model enabled stakeholders in Eswatini to determine the current cybersecurity status and posture for Eswatini, and highlighted a range of challenges and opportunities that Eswatini needs to seek or address in this strategy.

1.3.1 Summary of the Key Findings of the Assessment as of September, 2017

i) Although Eswatini has started considering cyber security as a priority issue in its ICT policy implementation, there is no overarching national cyber security programme for the nation.

ii) Eswatini does not have a formal framework or approach for monitoring cyber threats; and detecting, preventing and mitigating cyber-attacks within the country.

iii) Eswatini has not formally identified Critical National Infrastructures (CNI) and categorised their respective Critical Information Infrastructures (CII). There is no formal collaboration framework between CII operators or owners and the Public Sector. In addition, there is no national risk management framework and contingency plans against cyber-attacks to ensure resiliency of CIIs.

iv) Eswatini does not have adequate and effective legislation, policies and regulations on cyber security, which are required to address both current and future cyber security threats. A number of draft Bills addressing various cybersecurity issues are still being considered but haven't been formally enacted.

v) There is inadequate training capacity and lack of specialised expertise in Cybersecurity both public and private sectors in Eswatini.

vi) In general, there is limited awareness of cybersecurity and how to mitigate cyber-attacks and this is exacerbated lack of a cybersecurity mind-set and culture across all segments of society in Eswatini.

1.4 National Cybersecurity Strategy Alignment with National Agenda

This strategy is aligned with the objectives and aspirations of the national agenda of Eswatini

- National Development Strategy (Vision 2022) of the Kingdom of Eswatini which is aimed at creating by 2022 a nation which "will be in the top 10% of the medium human development group of countries founded on sustainable economic development, social justice and political stability" by focusing on addressing the quality of life in the country.

The critical dimensions of the quality of life as targeted in Eswatini Vision 2022 include poverty eradication, employment creation, gender equity, social integration and environmental protection.

- His Majesty's Government Programme of Action 2013 – 2018 which outlines the steps that the Government will take, through best service delivery, to improve the prosperity of Swazis for the period of 2013 – 2018.

- National Information and Communication Infrastructure (NICI) Implementation Plan which is aligned to the NICI Policy Vision "To harness ICT infrastructure and ICT solutions that enhance the building of a truly Twenty-First Century Kingdom of Eswatini with sustainable socio-economic development, accelerated poverty reduction, equal opportunities for all regardless of gender and physical ability" and ICT sector goals for the following Priority Areas: Human Resource capacity, Infrastructure Development, Education, Strategic ICT Leadership, Financial Services Sector, ICT Industry, Legal/Regulatory Frameworks, Environmental Management, and Media.

- The e-Government Strategy for Eswatini: 2013 to 2017, which sets out the framework for e-government and m-government in Eswatini, and outlines both "e" (electronic) and "m" (mobile) government initiatives.

- The SADC Integration Agenda which focuses on: "Promotion of sustainable and equitable socio-economic growth, Promotion of common political values and the Promotion, consolidation and maintenance of democracy, peace and security" and the vision to achieve a 'Digital SADC' by 2027

This Strategy will support the attainment of the desired outcomes of the abovementioned Strategy and Policy instruments by ensuring that Eswatini fully leverages its cyberspace to support and enhance prosperity and wellness of its citizens across all segments of its economy and society.

Eswatini is in the process of establishing a number of regulatory and legislative instruments, which will provide direction and guidelines on a number of key cybersecurity related issues.

Although there is currently no legislation specifically addressing cybersecurity, the current framework for cybersecurity, which provides some direction and governance on secure e-commerce, e-transactions and cryptology services are catered for by:

  - *Electronic Records (Evidence) Act 2014, which gives legal effect to: admission and authentication of electronic records; evidence of electronic records;*

including secure electronic records; and admissibility of electronic signature and integrity of electronic record

- *Cryptography Regulations (published in the latter half of 2016)*

- Electronic transactions is provided for by:
  - *Electronic Communications and Transactions Bill*

- Data protection and online privacy is provided for by:
  - *Data Protection Bill, which is still awaiting enactment by parliament*

- Cybercrime is provided for by:
  - *Computer Crime and Cyber Crime Bill, which is still awaiting enactment by parliament*

2 STRATEGY APPROACH

The National Vision for cybersecurity together with the core elements of Eswatini's approach for managing the numerous cyber threats are outlined in this section.

2.1 Vision Statement

Eswatini's Vision for Cybersecurity is:

"A safe, secure and resilient Cyberspace in Eswatini"

2.2 Strategic Goals

Eswatini aims to achieve the above National Vision through the following five key Strategic Goals:

- ***Strategic Goal 1****: Enhance the security and resilience of national critical information infrastructure and other related ICT services*
- ***Strategic Goal 2****: Strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini*
- ***Strategic Goal 3****: Build Eswatini's capacity and expertise in cybersecurity*
- ***Strategic Goal 4****: Foster a safe and secure information society for Eswatini*
- ***Strategic Goal 5****: Strengthen cooperation, collaboration and partnerships on cybersecurity*

2.3 Guiding Principles

The execution of this strategy will be underpinned by the following principles:

1. ***The Rule of Law:*** This Strategy will be implemented in accordance with the laws recognized in Eswatini and enshrined in Eswatini Constitution (2005), which protects the fundamental rights and freedoms of all citizens. This Strategy will also be implemented in accordance with international instruments, which Eswatini has ascended to such as the Articles 16, 17(e) and 34(c) of the UN Convention on the Rights of the Child.
2. ***Shared Responsibility:*** Eswatini recognises that all stakeholders have their individual roles and responsibilities in protecting Eswatini's cyberspace. This strategy will ensure that all stakeholders in Eswatini meet their responsibilities in protecting and enhancing resilience and availability of all the CIIs in Eswatini. This strategy will also

provide a platform for all stakeholders to collaborate and cooperate with each other in order to have an equitable shared responsibility.

3. ***Risk-based approach:*** The Kingdom of Eswatini fully appreciates that it is nearly impossible to ensure complete cyber security across the nation, and that is why, this Strategy will ensure that individuals and institutions in Eswatini employ a risk based approach in prioritising and executing cyber related activities, as well as assessing and managing cyber threats.

4. ***Universal Access to Internet and Cyberspace:*** This Strategy will ensure that all individuals and organisations within Eswatini have full access to the Internet, and are able to fully leverage a secure cyberspace to improve their prosperity and wellness.

5. ***ICT as a key enabler:*** Eswatini recognises that digitisation of nations tends to translate into improvement in social-economic prosperity and wellbeing of its citizens. In order to achieve this, Eswatini has embarked on embracing ICTs as a key enabler for social and economic development. This strategy will support this transformation by ensuring that cybersecurity becomes an integral consideration of all strategies, programmes and capabilities deployed by Eswatini to enable digital transformation.

6. ***Proactive action:*** Eswatini will proactively develop the requisite measures and tools to detect and manage the constantly evolving cyber threat landscape. It will also encourage individuals and organisations in Eswatini to proactively defend their information systems, data and networks.

3 ACHIEVING STRATEGIC GOALS

The following section outlines the Specific Objectives and Strategies that need to be achieved and executed respectively, to enable the attainment of Eswatini's national Vision on Cybersecurity by 2025. These Strategies will be executed in a manner that is consistent with the principles described above.

3.1 *Strategic Goal 1:* Enhance the security and resilience of national critical information infrastructure and other related ICT services

As Eswatini embarks on digitally transforming its economy and society, more and more processes and services across Eswatini are increasingly becoming reliant on ICT systems and networks, and data that is generated or accessed by these systems. This dependency implies that any successful attack on some of these systems can severely impact the socio-economic wellbeing of the citizens of Eswatini. This will result in the lack of services supported by the Critical Information Infrastructure, which enables delivery of essential services across the nation like electricity, healthcare, transport etc., as well as information systems that support the well-functioning of the Eswatini society like e-government services and financial services.

Eswatini acknowledges that the digital transformation of its economy and society should include, as a priority, the protection of CII and other ICT related services. The relevant MDAs in government will work with all relevant organisations to protect and enhance the resilience of CIIs including e-Government and other related ICT services, especially as most of these systems are owned and operated by the private sector. Eswatini will ensure that all relevant stakeholders understand their roles and responsibilities in protecting CII and ICT services.

3.1.1 Specific Objective 1.1: Protect the critical information infrastructure and other ICT related services

Both public and private sector organisations, particularly their senior directors and board level management, that own and manages most CIIs as well as other ICT related services, must fully understand their systems, networks and data. These organisations will be expected to identify their critical information systems, regularly monitor these systems to detect and manage vulnerabilities and threats. Eswatini will provide oversight and intervene where necessary to ensure that these organisations develop the necessary capabilities to be resilient from attacks. This is in addition to managing cyber threats, risks, and vulnerabilities across all CIIs and relevant ICT services in Eswatini. There is a need to foster a thorough

understanding of the vulnerabilities and threats facing CIIs and ICT services across Eswatini, and ensure that effective measures are implemented, which will improve the cybersecurity of these CIIs and ICT services.

Actions:

3.1.1.1 Establish a National Critical Information Infrastructure Register.

3.1.1.2 Develop a national CII Governance Framework, which describes CII protection procedures, processes, guidelines, good practices to be adhered to by CII Operators and owners.

3.1.1.3 Establish a National Risk and Vulnerability Register and Regulations, to ensure continuous vulnerability monitoring and disclosure as well as risk assessment and management across all CIIs.

3.1.1.4 Develop and continually review CII minimum security standards and procedures to be complied with, including security audits, equipment specifications, Standard Operating Procedures (SOPs), Access Control Mechanisms, etc.

3.1.1.5 Conduct continuous monitoring of, and regular testing of CII and Information Systems to detect vulnerabilities, illicit access, errors, etc.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.1.1.6 The Government of Eswatini together with CIIs and ICT services owners across Eswatini will keep abreast of, and fully understand the vulnerabilities, risks and levels of cyber security across CII and Information Systems in Eswatini.

3.1.1.7 Eswatini will ensure there is resilience and availability of CIIs and ICT services across Eswatini, following the establishment and implementation of appropriate CII protection measures.

3.1.1.8 CII and Information Systems operators have an improved capacity to manage cyber threats and incidents.

3.1.2 Specific Objective 1.2: Manage cyber threats facing Eswatini

Consistent with global trends, which indicate that the number and severity of cyber incidents affecting individuals and organisations across nations, including Eswatini, will grow, coupled

with the rapidly evolving cyber threat landscape. Eswatini appreciates that it will need to enhance the managing of cyber threats. It will also have to increasingly provide support to organisations across all sectors on how to manage these threats. This will involve, inter alia, contributing to the detection and mitigation of cyber threats, as well as the gathering and dissemination of information about current and emerging cyber threats nationwide. This will also require Eswatini to work closely with the private sector and other partners such as regional SADC countries to ensure an effective, efficient and coordinated cyber incident response framework across the region.

Actions:

3.1.2.1 Define, publish and continuously review the minimum incident register requirements to enable dependable incident analysis against a rapidly evolving cyber landscape.

3.1.2.2 Continuously identify, monitor and analyse risks and cyber threats in order to provide a real-time picture of the threats and risks facing Eswatini.

3.1.2.3 Develop and continuously update a national cyber incident register for Eswatini.

3.1.2.4 Continuously analyse cyber incidents within Eswatini and the SADC region to develop and execute measures to resolve incidents and manage cyber threats.

3.1.2.5 Develop and implement national procedures for risk management and data protection.

3.1.2.6 Develop and continuously update cyber incident scenarios and cyber contingency plans that clearly define crisis management procedures including the roles and responsibilities of all stakeholders during cyber incidents and emergencies, and which can be used during cyber exercises.

3.1.2.7 Undertake regular cyber drills and exercises to test national crisis management measures, and leverage lessons learned to improve crisis management measures and the national response to cyber incidents.

Desired Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.1.2.8 With its comprehensive understanding of cyber threats, Eswatini will establish and implement a national and synchronized cyber incident management approach.

3.1.2.9 Eswatini will establish a centralised incident reporting and response functionality within the National Cybersecurity Agency and as result cyber incidents are regularly and consistently reported to Eswatini's National Cybersecurity Agency.

3.1.2.10 Through its National Cybersecurity Agency, Eswatini will be able to effectively and efficiently manage cyber incidents nationwide.

3.2 *Strategic Goal 2:* Strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini ICT services

Given the cross border nature of cyber threats and the potential for causing significant damage, if successful, it is imperative that Eswatini implements robust cybersecurity governance structures; have relevant policies, regulations and legislation. These will provide all relevant stakeholders, particularly private and public institutions with a wide set of tools to ensure effective cybersecurity governance and management across Eswatini. This will require establishment of clearly defined processes, functions, policies, responsibilities and roles, to ensure effective disruption of cyber criminal activities targeting Eswatini, as well as the effective management of potential cyber threats. These frameworks should also enable the country to fully benefit from the opportunities provided by cyberspace and the on-going digital transformation.

3.2.1 Specific Objective 2.1: Establish a cybersecurity institutional framework to ensure the effective management of cybersecurity across Eswatini

With increasing sophistication of cyber criminals and prevalence of cyber threats, it is paramount that Eswatini sets up a comprehensive cybersecurity institutional framework for the kingdom. This institutional framework will promote and facilitate effective and rapid coordination of cybersecurity activities in a coordinated manner. The framework will also enable Eswatini to provide effective governance and leadership on cybersecurity and related issues. This will also ensure that stakeholders avoid duplication of efforts and inconsistencies when discharging their respective responsibilities. In addition, such a framework will ensure that Eswatini has the ability to respond to cyber threats, and protect CIIs and ICT services in the country.

National Cybersecurity Agency - In order to have a coherent and comprehensive institutional framework, some of its functions will include: - coordination of the implementation of this strategy and related initiatives; coordination of national cyber incident detection, prevention and response; periodic review and updating of this Strategy. Eswatini aspires to establish a National Cybersecurity Agency (NCA), with legitimate mandate, legal authority, relevant skills/expertise, and capabilities required to lead on cybersecurity related issues and its implementation in Eswatini. The NCA will be housed and function under the

Communications regulator, ESCCOM, and work along with law enforcement agencies and national security, other relevant institutions in coordination with the Ministry of ICT.

National Cybersecurity Council – this is an executive level body that will be made up of Ministry of ICT, ESCCOM, Police, Ministry of Justice, Ministry of Foreign Affairs, Defence, Financial Services Sector, Operators, Academia, Civil Society. This is an advisory body under the office of the Prime Minister. This body will oversee the overall cybersecurity posture of the country and it will meet at least two times a year and advise Government. The chairman will be appointed by the Prime Minister and the National Cybersecurity Agency will serve as the secretariat. In the absence of the NCA, Director Communications serves as the secretariat.

Cybersecurity Working Groups – These are working groups formed from technical people to work under the guidance of the Ministry of ICT. They may consist of personnel from institutions such as CII operators, ISPs, academic institutions, prosecutors, police, government, etc, who deal with issues of cybersecurity on a daily basis one way or another. These are the Awareness and Capacity Building Aspects Group; the Policy, Legal and Regulatory Aspects Group; the Technical Aspects Group; the National Security Aspects Group and the Institutional and Governance Aspects Group. They work under the guidance of the Director of Communications. Such groups are flexible and may be reconstituted as the environment demands.

Actions:

3.2.1.1 Create and operationalize the National Cybersecurity Agency of Eswatini with the mandate for developing, implementing and coordinating cybersecurity initiatives in Eswatini, and provide leadership on the implementation of this strategy

3.2.1.2 Create the Cybersecurity Working Groups to help in the implementation of the strategy.

3.2.1.3 Create the national CERT/CSIRT as a department within the National Cybersecurity Agency with clear functions and responsibilities including incident response.

3.2.1.4 Establish a National Cybersecurity Training & Research Unit within the Innovation Park at RSTP and other institutions.

3.2.1.5 Create the National Cybersecurity Council.

3.2.1.6 Establish a National Cyber Defence Command Centre for Eswatini.

3.2.1.7 Strengthen the role and mandate of law enforcement and security agencies to enhance their capacity in various areas including digital forensics, digital evidence and other computer enabled methods to disrupt malicious cyber activities.

3.2.1.8 Develop a cyber defence strategy, which describes the national approach for addressing cyber threats to the national security of Eswatini.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.2.1.9 Eswatini will establish a centralised and robust governance framework that has at its core, a coherent and national approach for developing, implementing and coordinating initiatives relating to cybersecurity in Eswatini.

3.2.2 Specific Objective 2.2: Establish and articulate the national position on cybersecurity

It is critical that Eswatini establishes and articulates its national position on cybersecurity issues to ensure coherent and seamless interactions of public and private organisations within Eswatini. In articulating its national position on cybersecurity, Eswatini aims to ensure it is innovative and creative, outward and forward looking (i.e. considers factors within and beyond Eswatini).

Desired Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcome:

3.2.2.1 Eswatini will have a clear and coherent position on cybersecurity that is understood by all stakeholders and will drive the national focus in ensuring a safe, secure and resilient Cyberspace for Eswatini.

3.2.3 Specific Objective 2.3: Establish a comprehensive legal and regulatory framework for cybersecurity

The on-going efforts by Eswatini to leverage ICTs as an enabler for socio-economic development, and the benefits from improved prosperity and wellness resulting from digitising its society and economy, will increasingly face Cyber threats perpetrated through sophisticated cybercrimes. In addition, and considering that the global cyber threat landscape and cyber trends are rapidly and continuously changing, Eswatini will need to establish, and continuously review cybersecurity legal and regulatory frameworks that are aligned and relevant to current and emerging cyber trends. These frameworks will provide all relevant stakeholders, such as the judiciary and law enforcement agencies, with the appropriate technology and tools to enable them to carry out their mandate effectively.

Eswatini will prioritise the enactment and enforcement of all relevant cybersecurity laws that are currently pending, including: - the *Computer Crime and Cybercrime* Act, the *Data*

Protection Act and other appropriate instruments to strengthen provisions addressing various cybersecurity issues. These provisions or instruments also need to be aligned to both regional (with SADC) and international norms (including the Budapest convention), criminalise malicious cyber activities in Eswatini, and improve the investigation and prosecution of cybercrimes. It is important that the established cybersecurity legal and regulatory framework for Eswatini is suitably applicable and technology neutral. This will enable Eswatini to tackle emerging cyber threats effectively whilst still allowing innovation and growth of the ICT sector.

Actions:

3.2.3.1 Expedite the enactment of pending legislation relating to Cybersecurity.

3.2.3.2 Undertake a gap analysis of Eswatini's Legal and Regulatory Framework in order to identify gaps related to cybersecurity. Once identified, establishing appropriate instruments to address these gaps as well as enhance Eswatini's legal and regulatory framework on cybersecurity and cybercrime.

3.2.3.3 Subscribe to relevant regional and international instruments relating to cybersecurity and cybercrime.

3.2.3.4 Review and improve legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to enhance the fight against cybercrime.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.2.3.5 Establish an updated and forward-looking legal and regulatory framework, which addresses on-going developments and trends in relation to cybersecurity, and includes relevant international standards that will enhance Eswatini's capability to combat cybercrime activities targeting or committed in Eswatini.

3.2.3.6 Have a comprehensive and robust legal and regulatory framework, which provides Eswatini's law enforcement and judiciary with the appropriate tools and technologies to execute their mandate with respect to cybersecurity and cybercrime.

3.2.4 Specific Objective 2.4: Establish cybersecurity standards, guidelines, technical and operational frameworks

Eswatini will ensure that various instruments including cybersecurity standards, guidelines, technical and operational frameworks are developed, published and deployed nationwide. These frameworks will ensure that both public and private organisations including individuals

nationwide understand their responsibilities in securing their data, information systems and networks, based on good cybersecurity practices and measures. Eswatini will ensure that these standards, guidelines, technical and operational frameworks are tailored to national specifications that will enhance the cybersecurity posture for Eswatini, especially with respect to the CIIs and ICT services.

Actions:

3.2.4.1 Develop and promote the adoption of a National Cybersecurity Standards Framework across CIIs and ICT services in Eswatini.

3.2.4.2 Promote the awareness and implementation of a National Cybersecurity Standards Framework across the private sector, especially the Small and Medium Enterprises (SME) sector which contributes significantly to Eswatini's economy.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.2.4.3 Establish comprehensive and appropriate cybersecurity standards, guidelines, operational frameworks, processes, procedures applicable to Eswatini, and as a result, secure CIIs and ICT services based on well-defined national cybersecurity standards.

3.3 *Strategic Goal 3*: Build Eswatini's capacity and expertise in cybersecurity services

Eswatini requires a skilled and talented human resource pool to in order to drive the digital transformation of Eswatini in a manner that ensures the resilience and availability of CIIs and ICT services, and fosters confidence and trust in cyberspace across the nation. This is a key motivation of this strategy, which seeks to ensure a rapid development of qualified and talented cybersecurity professionals nationwide by addressing the existing challenges limiting the development of cybersecurity capacity and expertise in Eswatini. Some of these challenges include:

- lack of funding and support for cybersecurity capacity building especially in the public sector,
- shortage of locally based cybersecurity trainers,
- lack of career and training pathways,
- insufficient cybersecurity training and education programmes,

- limited focus on cybersecurity in the national curricula.

Eswatini will promote collaboration and cooperation among all relevant stakeholders in the development and execution of various measures aimed at tackling these existing barriers. A number of stakeholders have been identified including:

- relevant government ministries, departments and agencies;
- schools, universities, private sector organisations, academia, and
- civil society among others.

3.3.1 Specific Objective 3.1: Develop a nationwide and sustainable pool of highly skilled cybersecurity professionals

Eswatini will embark on addressing the current lack of cybersecurity skills and expertise nationwide, by establishing a national approach for developing skills and expertise on cybersecurity across Eswatini. This approach will consist of a number of measures aimed at transforming cybersecurity education and training across Eswatini, and will be underpinned by the recognition of the collective role and responsibility of multiple stakeholders such as the government, education sector, both private and public sector, civil society, and the academia in addressing the skill shortage.

Eswatini will undertake an assessment of the current situation in relation to availability of cybersecurity skills or expertise nationwide, and develop a coherent strategy to increase both the number and diversity of qualified cybersecurity professionals trained through the national education system. This will enable Eswatini to have the appropriate skillset and numbers to meet both its current and future cybersecurity needs. Eswatini will promote collaboration among all relevant stakeholders including the education sector, private and public sectors, and other relevant sectors and civil society to

- enhance cybersecurity education nationwide;
- develop career and education pathways;
- support cybersecurity R&D;
- and create cybersecurity internships.

This will in turn improve current interest in the cybersecurity profession, and enhance the capacity of cybersecurity experts able to tackle current and emerging cybersecurity threats and challenges.

Actions:

3.3.1.1 Develop a National Cybersecurity Education and Career Scheme aimed at promoting careers and continuous educational training in cybersecurity

3.3.1.2 Review and update the current education curriculum and related materials education system in Eswatini and introduce cybersecurity aspects/concepts.

3.3.1.3 Promote collaboration among universities, tertiary colleges and the private sector to create internships/studentships and work experience programs in cybersecurity.

3.3.1.4 Define minimum standards in cybersecurity training and education qualifications in Eswatini.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.3.1.5 Cybersecurity becomes a core component of Eswatini's national curriculum, and taught at all levels of the education system, resulting in a sustained pool of cybersecurity professionals.

3.3.1.6 Increased interest in cybersecurity profession by a wide range of individuals in Eswatini.

3.3.1.7 Cybersecurity will constitute a major component of continuous professional development programmes for all professionals.

3.3.2 Specific Objective 3.2: Build technical skills and capacity in cyber resilience and incident response

Eswatini will develop and execute a national cybersecurity capacity building strategy which will create and increase availability of technically skilled work force and capacity in cyber resilience and incident response across all relevant segments of Eswatini's economy. This will consist of driving a great increase in the number of professionals nationally who possess the technical skills and capacity to successfully undertake national preparedness, response and recovery activities necessary to face cyber incidents and ensure the resilience of data, systems, and networks across Eswatini. This will also require continuous training and education of staff of various relevant organisations responsible for national response to cyber incidents.

Actions:

3.3.2.1 Assess the capacity and expertise of the National Cybersecurity Agency and other relevant public institutions to identify and address gaps/weaknesses in skills.

3.3.2.2 Train and educate CERT/CSIRT Staff and other relevant government institutions to develop their skills and capacity to manage cyber threats and cyber incidents effectively, particularly national cyber incident preparedness, response and recovery activities.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.3.2.3 Organisations across Eswatini, including the National Cybersecurity Agency has the requisite technical skills and capacity to effectively manage cyber threats and cyber incidents nationally

3.3.3 Specific Objective 3.3: Build the technical skills and capacity required to investigate and prosecute cybercrimes, and effectively enforce established cybersecurity legal and regulatory instruments in Eswatini

Eswatini will ensure that law enforcement agencies including the Royal Eswatini Police Service, the Intelligence Service of Eswatini and other relevant agencies continuously improve their capacities and capability to effectively detect, investigate, prosecute and disrupt cyber criminal activities targeting individuals and organisations in Eswatini. Eswatini will ensure that all relevant stakeholders collaborate to develop and enhance capacity and capabilities for effective enforcement of established Cybersecurity laws and related regulations in Eswatini.

Actions:

3.3.3.1 Continuously train and educate law enforcement agencies and the judiciary to develop and enhance their capacity and capability to enforce the cybersecurity related provisions of the legal and regulatory framework, including investigation and prosecution of cybercrimes.

3.3.3.2 Conduct digital forensics and evidence handling courses for all relevant agencies involved to enhance detection, investigation and prosecution of cybercrimes.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.3.3.3 Improved understanding among relevant stakeholders of the cybersecurity provisions of the legal and regulatory frameworks, consistently and effectively enforced resulting in more successful detection, investigation, prosecution and disruption of cyber criminal activities.

3.3.3.4 Enhanced capacity and capability of law enforcement agencies and other relevant stakeholders to disrupt, investigate and prosecute cyber criminal activities targeting Eswatini both nationally and internationally.

3.3.4 Specific Objective 3.4: Foster Innovation and Research & Development (R&D) in cybersecurity

Eswatini will create an enabling environment to enable innovation and research & development in the area of cybersecurity in Eswatini. This will involve supporting skills development and encouraging investment in Cybersecurity. Eswatini will also ensure a widely available and easily accessed funding for cybersecurity professionals and organisations involved in research and development of cybersecurity services and products in Eswatini. This will leverage the Innovation Park of RSTP and other institutions to drive innovation and R&D, and support organisations and individuals or start-ups conducting R&D in cybersecurity.

Actions:

3.3.4.1 Promote and support cybersecurity competitions and R&D projects in Universities, Colleges and Schools.

3.3.4.2 Establish a national funding and incentive programme to support national enterprises providing Cybersecurity solutions.

3.3.4.3 Establish partnerships between education sector, public and private sector, and international partners to enable Eswatini individuals and organisations to take part in national and international cybersecurity capacity building and R&D activities.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.3.4.4 Increase in investment in Cybersecurity innovation and R&D in Eswatini, particularly towards the local cybersecurity service providers, resulting in year-on-year growth in the cybersecurity posture for Eswatini.

3.3.4.5 Eswatini proactively supports national cybersecurity service providers through various measures including selective government procurement, contracts, and other incentives.

3.4 *Strategic Goal 4*: Foster a safe and secure information society for Eswatini

Eswatini will work closely with all relevant stakeholders to strengthen their understanding and awareness of cyber threats facing them, and in the process effect positive changes towards Cybersecurity good practices. There is inconsistency across various sectors in adopting and executing appropriate steps in protecting their data, information systems and networks in Eswatini. While both the Telecommunications and Financial sector in Eswatini have internal cybersecurity awareness programmes and taken various measures to protect their infrastructures, a significant number of organisations and individuals in Eswatini are yet to adopt good practices in enhancing Cybersecurity. Eswatini will roll out a number of measures and initiatives to change the behaviours of individuals and organisations across Eswatini such that they become cybersecurity conscious, adopt and implement appropriate good practice measures to protect themselves online and against cyber threats, thereby creating a secure and safe information society in Eswatini.

3.4.1 Specific Objective 4.1: Establish a cybersecurity mind-set and culture in Eswatini

Eswatini will roll out a number of measures, which will create a cybersecurity mind-set and culture across the nation. These measures will be based on a nationwide study to assess the reasons preventing individuals and organisations in Eswatini from adopting a cybersecurity mindset and culture. These measures will also include tailored awareness raising campaigns targeting specific groups of individuals and organisations. Eswatini will use a wide range of channels to rollout these awareness programmes including social-centres, billboards, communities, media, etc. In addition, Eswatini will work with a range of stakeholders including relevant entities in Eswatini that regularly engage with citizens like known civil society organisations and relevant government agencies. Eswatini will also seek to understand the financial impacts of managing cyber threats and risks, particularly within the Eswatini context and disseminate this information widely.

Actions:

3.4.1.1 Conduct a national study to assess levels of Cybersecurity awareness across Eswatini. Then develop and roll-out tailored national awareness programmes targeting all groups of users, especially those who are vulnerable and at risk such as children, women, seniors citizens and other vulnerable groups

3.4.1.2 Publicise cybersecurity good practices nationwide to instil a cybersecurity culture across Eswatini.

3.4.1.3 Conduct mandatory cybersecurity training of high-ranking government officials, legislators, private sector board members and management.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.4.1.4 Cybersecurity good practices are widely established both in private and public sectors across Eswatini, resulting in continuous reduction in the number of serious and high-impact cyber-attacks in Eswatini.

3.4.1.5 Organisations and individuals in Eswatini, especially high ranking government officials, legislators, private sector board members and management, understand the need for cybersecurity, responsibilities, liabilities, together with the measures for protecting their organisations establishment of a cybersecurity culture in Eswatini.

3.4.2 Specific Objective 4.2: Create a secure environment for e-government services in Eswatini

Eswatini is committed to rollout e-government services across all segments of its economy and society. This will require embedding minimum levels of cyber security for e-government and e-commerce services, which will in effect build trust and confidence in e-government services among all users. The Kingdom of Eswatini will embark on addressing the risks that face e-government and e-commerce services including risks relating to confidentiality of data of users and organisations. This will involve setting out measures: that ensure the integrity of data to provide assurances that data has not been illicitly tampered, or illicitly accessed by unauthorised parties, just to list a few. The Kingdom of Eswatini will accelerate the rollout of IPv6, Public Key Infrastructure (PKI) and minimum security baselines in the design and execution of e-government services.

Actions:

3.4.2.1 Deploy PKI across the nation especially in e-government services so as to leverage the security features of PKI relating to confidentiality, authentication and data integrity.

3.4.2.2 Encourage the transition from IPV4 to IPV6 protocol to leverage the IPV6 security features relating to confidentiality, integrity and authenticity of information data.

3.4.2.3 Ensure mandatory or minimum security requirements are considered during the development of e-government services.

Expected Outcome: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.4.2.4 Eswatini's e-government services are underpinned by cybersecurity requirements, baselines and functionality, and as a result are trusted and used with confidence by organisations and individuals in Eswatini.

3.4.3 Specific Objective 4.3: Build trust in the use of e-government services

To spur widespread adoption and utilisation of e-government services nationwide, Eswatini will have to build trust among individuals and organisations. This will require the provision of easily understandable information to users on the security features of these services. Consequently, users will make informed choices and decisions about utilising e-government services and eventually build up trust and confidence in these services. Eswatini will prioritise the provision of information on the built-in security features of e-government services used across the nation. Eswatini will also seek to understand security-related concerns of individuals and organisations in relation to e-government services and deploy measures to address these concerns. The National Cybersecurity Agency will be designated to collect and analyse information on various security concerns expressed across Eswatini, analyse whether current security features address these concerns, and develop appropriate features where necessary. This information, analysis and measures will be disseminated across the nation in a format and language that is easily understandable. Eswatini will foster effective communication between all relevant stakeholders to demonstrate how secure e-government services are, thereby building trust and enabling citizens to make informed choices and decisions based on the extent of in-built security of these services.

Actions:

3.4.3.1 Establish Points of Contact within the National Cybersecurity Agency who will interface with individuals and organisations across Eswatini to collect information on their security concerns with e-government services, and analyse how these concerns have been addressed or resolved.

3.4.3.2 Publicise widely and regularly across Eswatini how e-government services have been secured to build trust in the use of e-government services and Eswatini's cyberspace in general.

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.4.3.3 Robust and secure e-Government services deployed across Eswatini. Deploy security measures to address comprehensively concerns expressed by users of e-government services and disseminate widely information gathered on how these concerns have been addressed.

3.5 *Strategic Goal 5*: Strengthen cooperation, collaboration and partnerships on cybersecurity

Taking into account the borderless nature of cyberspace, Eswatini fully understands that it is crucial for it to collaborate with international stakeholders to ensure a safe and secure cyberspace. Eswatini will build on existing cooperation and collaboration frameworks to take part in cybersecurity activities and debates taking place beyond Eswatini. These opportunities will enable Eswatini to address cyber issues, and create a secure and open cyberspace to enhance the prosperity of the citizens of Eswatini. This participation should result in a marked decrease in the cyber risks, threats and malicious activities, especially originating beyond Eswatini's borders.

3.5.1 Specific Objective 5.1: Promote collaboration and information sharing on cybersecurity

Eswatini considers information sharing and collaboration as a key pillar for addressing cybersecurity related challenges. Eswatini will establish a framework that ensures rapid information sharing between stakeholders, particularly between the government and private sector to ensure that all stakeholders are informed regularly and timely on particular cyber threats or attacks. Eswatini envisages that its national CERT/CSIRT unit will serve as a centre of information sharing activities across Eswatini, and will ensure that wide dissemination and awareness of information on vulnerabilities, incidents and mitigation efforts across the Eswatini. In addition, this also fosters a trusted and collaborative learning environment where stakeholders develop a deeper understanding of emerging cyber threats, risks and mitigation techniques, and benefit from effective information sharing and collaboration.

Actions:

3.5.1.1 Establish a network of sectorial cybersecurity focal points together with an information sharing framework to enhance collaboration and mutual exchange of information on Cybersecurity locally and internationally

3.5.1.2 Mandate the National Cybersecurity Agency as the national body for overseeing information sharing and collaboration on cyber security.

3.5.1.3 Create national fora to promote a national information sharing on cybersecurity

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.5.1.4 Eswatini has more effective information sharing on cybersecurity issues both locally and internationally, which in effect translate to more effective management of cyber threats nationally.

3.5.2 Specific Objective 5.2: Establish partnerships to promote collaboration and cooperation in addressing cybersecurity issues locally and internationally

Considering the rapidly changing cyber threat landscape, and the cross border nature of cyberspace, Eswatini appreciates that stakeholders, whether national or international, benefit from working together to tackle cybersecurity issues locally and internationally, especially in leveraging the unique but often times complementary strengths of both sectors. For instance, within Eswatini, the private sector largely own and operate the critical information infrastructure of Eswatini, and as such has already developed specific skills and capacity in addressing cyber threats. While, the public sector notably, law enforcement agencies, are better positioned to investigate and prosecute cyber-criminal activity or liaise with other international agencies or nations to access and act upon intelligence on cyber-criminal activity. The Kingdom will embark on facilitating the establishment of partnerships:

- To enable the identification or detection of criminal behaviour or behaviours of concern;
- To facilitate the adoption of, and adherence to established good practices of cybersecurity;
- To enable nationwide responses to cyber threats; and
- To ensure that emerging cybersecurity developments and implications to the nation are fully understood by all stakeholders, notably the government.

Actions:

3.5.2.1 Develop an International Collaboration Strategy that outlines how international collaboration on cybersecurity and cybercrime is managed and funded

3.5.2.2 Enhance partnerships with local partners, other states and international stakeholders to collaboratively address cyber security and combat cybercrimes

Expected Outcomes: In executing these strategic objectives, Eswatini expects to achieve the following outcomes:

3.5.2.3 Effective collaboration with all relevant stakeholders on cybersecurity issues, and active participation in international cybersecurity activities, resulting in improved management of cyber threats and disruption of cyber criminal activity targeting and/or originating from Eswatini.

4 IMPLEMENTATION AND MANAGEMENT

4.1 Roles and Responsibilities

It is imperative that a collective understanding and recognition of the shared responsibility of all stakeholders in protecting the CIIs and ICT services in Eswatini is at the core of the management and implementation of this Strategy. Hence the delineation of roles and responsibilities of key stakeholder groups in Eswatini is described as follows:

The Government of Eswatini is responsible for ensuring the protection of the national cyberspace and citizens of Eswatini. Consequently, within the context of this Strategy, the Government will be responsible for managing the cyber threats targeting the critical information infrastructure and national security of Eswatini. Bearing in mind that the Government of Eswatini holds national data and provides e-government services to citizens and organisations, it is crucial that the Government of Eswatini puts in place robust and appropriate measures to protect the systems, networks and information it possesses and manages. While some CII are owned and operated by the private sector, the Government of Eswatini is still responsible for ensuring that all CII in Eswatini are resilient and able to support the continuous supply of essential services in Eswatini. This will require the Government to ensure all CII service providers comply with minimum security standards for CII. Another key responsibility of the Government of Eswatini includes the provision of information and advises to individuals and citizens thereby enabling them to adopt and implement the appropriate measures for protecting themselves. One crucial role and responsibility of the Government relates to the fostering an enabling environment for cybersecurity, where Eswatini's education and training system produces a sustainable pool of cyber expertise which will in turn drive an innovative and vibrant cyber sector in Eswatini. In effect, the Government of Eswatini is responsible for ensuring the successful implementation of this Strategy and the attainment of the Expected Outcomes for the nation vis-à-vis cybersecurity.

Eswatini will establish a **National Cybersecurity Agency** to lead the implementation of this Strategy. Consequently the National Cybersecurity Agency will coordinate, plan and implement cybersecurity initiatives across Eswatini. The National Cybersecurity Agency through its dedicated **National CERT/CSIRT** Unit will lead the cyber incident response and management activities of Eswatini at the national level. The Agency will also oversee the protection of CII in Eswatini, and provide advice and support to organisations across the nation. One key role and responsibility of the Agency will be the assurance of adoption and compliance of nationally established guidelines, standards, good practices, and security requirements necessary for the protection of the systems, networks, and data. In effect, the Agency will serve as the national source for cyber security expertise and direction nationwide.

Eswatini will constitute the **National Cybersecurity Council** and the **Cybersecurity Working Groups** with representatives from the public and private sector organisations, to provide strategic advice to Government.

Organisations based in Eswatini own and manage systems, networks and information in their day-to-day operations and provision of services. As a result, organisations are responsible for securing the systems, networks and information they own or manage, whilst ensuring the secure and continuous supply of services that are underpinned by these systems, networks and information. Consequently, organisations in Eswatini need to deploy appropriate investments and measures, and develop the right capacities to ensure the security and resilience of their systems, networks and information.

Owners and operators of **Critical Information Infrastructure and Information Systems** in Eswatini are responsible for ensuring the protection and resilience of their systems, networks and data, and will be required to execute all appropriate measures to ensure this protection and resilience. They will also need to make investments and roll-out measures that ensure their compliance with nationally defined cyber security guidelines, security requirements, standards, processes, procedures, frameworks, etc.

Royal Eswatini Police Service and the Judiciary in collaboration with other relevant stakeholders (national or international) will expand their efforts to disrupt, investigate and prosecute cyber criminal activity conducted in, or targeting Eswatini. The Royal Eswatini Police Service will work with the National Cybersecurity Agency to support the national cyber incident and cyber emergency responses.

The Umbutfo Eswatini Defence Force is responsible for ensuring the defence of Eswatini against cyber threats to the sovereignty and national security. This will require the Defence Force to manage threats directly under military jurisdiction including cyber warfare, cyber terrorism, etc. The Defence Force will be responsible for managing operations at the Cyber Defence Command Centre and for securing systems, networks, and data of the Defence Force. The Eswatini Defence Force will work with the National Cybersecurity Agency to support the national cyber incident and cyber emergency responses.

Civil Societies based in Eswatini will work with other relevant stakeholders in Eswatini to ensure the accountability and transparency of public and private sector organisations. They will also play a key role in building awareness of cybersecurity issues and trends nationwide and across all segment of the Eswatini society. Furthermore, they will facilitate, ensure and enhance engagement and dialogue among all stakeholders

All **Individuals** based in Eswatini will be responsible for adopting and implementing all appropriate measures to protect themselves online, and secure the systems, networks and data they own/or manage in their private and professional lives. It is critical individuals do this as they are potentially weak links in the cyber security of the nation, and could be an effective line of defence against cyber threats targeting Eswatini's collective data, networks and systems.

4.2 Approach for Monitoring and Evaluation

Taking into consideration the continually evolving cyber threat landscape, and to enable the successful implementation of this strategy, Eswatini will establish a Monitoring and Evaluation Plan which will enable it monitor progress and impacts of the recommended objectives and milestones in the Strategy. All monitoring and evaluation activities of Eswatini should enable the achievement of the national Vision and Strategic Goals of this Strategy by assuring the accurate reporting of progress, documentation of challenges faced, and the integration of lessons learned in on-going implementation activities.

Eswatini is committed to undertake monitoring and evaluation of this strategy in a manner that supports informed and effective planning and decision making. The Monitoring and Evaluation (M&E) Plan will ensure that the strategy is consistent with the following approach:

4.2.1 The M&E Plan will be based on well-defined SMART Performance Targets for each stakeholder group involved in, and responsible for implementing specific elements of this strategy.

4.2.2 The Plan will be based on annual action plans which establish a common understanding of the expected end results, outline the approach for achieving these end results and identify the resources required to achieve these end results. These annual action plans consider the Key Performance Indicators (KPIs), and Time Lines provided in the Implementation Logical Framework

4.2.3 It will specify performance and progress related indicators, and will establish who is responsible for collecting data on the indicators. The plan will also specify what methods and tools will be used to collect the data, and how the data will be used. The plan will be built on the Key Performance Indicators (KPIs), SMART Performance Targets and Time Lines.

4.2.4 It will ensure the progress in achieving expected results and Expected Outcomes is regularly monitored and reported on, with deviations promptly observed and reported as well.

4.2.5 The Monitoring and Evaluation Plan will ensure the periodic assessment of the performance against defined targets. These periodic reviews for determining progress in achieving Expected Outcomes and long term impact of strategy will be undertaken as follows

- Annual reviews
- Mid-term review at the start of year 3 of this strategy
- Long term review by end of the of year 4 of this strategy

4.2.6 The Plan will ensure that wherever necessary, remedial measures to keep implementation on track are adopted and implemented

Eswatini will develop and implement a detailed Monitoring and Evaluation Plan based on the proposed approach outlined above within 4 months of the launch of this strategy.

CONCLUSION

As Eswatini embarks on leveraging ICTs fully to digitally transform its economy and society, it acknowledges the existence of current cyber threats and on-going emergence of cyber threats amidst a global and rapidly evolving cyber threat landscape. Eswatini has developed this strategy, which clearly defines the national ambition, approach and commitment in ensuring that all current and future cybersecurity challenges and cyber threats are managed effectively and responsively.

Eswatini is dedicated to ensuring that the nation has the requisite capacity and capability to keep up and protect itself from future and current cyber threats. With the successful implementation of this strategy, Eswatini will transform itself into one of nations with a well-established cybersecurity posture, where harmful cybersecurity activity targeting or conducted in Eswatini is significantly disrupted and reduced, and individuals and organisations fully leverage cyberspace to improve their socio-economic prosperity and well-being.

To conclude, this Strategy provides the right tools to effectively integrate ICTs across all segments of Eswatini society and economy, which in turn will lead to significant transformation of wellness and prosperity of the Kingdom of Eswatini.

APPENDIX A - STRATEGY IMPLEMENTATION LOGICAL FRAMEWORKS

This section presents the key elements necessary to successfully implement the strategy:

- Strategic Goal: the substantive long term goal that Eswatini would like to achieve in each priority area;
- Specific Objective: the specific steps to be undertaken to achieve your Strategic Goal
- Strategies: The activities that must be undertaken, under this Strategic Plan, in pursuit of the Specific Objectives
- Deliverables/Outputs: The formal work products that Eswatini will achieve in the pursuit of the objectives and the implementation of the Strategy
- Lead Implementing Agency and Support: The Institutions with primary responsibility for managing completion of each objective, and the institutions that will provide support.
- Time Period: Period of time within which Deliverables/Outputs are produced and/or Strategies/Actions are implemented.
- Key Performance Indicators: The indices, data measurements, and trends that should be monitored to evaluate the progress in implementing the Strategy and achieving the objectives and Deliverables
- Possible Funding Sources and Mechanisms: An overview of different possible funding sources & mechanisms that can be adopted by Eswatini to fund the implementation of the NCS

Strategic Goal 1: Enhance ***the security and resilience of national critical information infrastructure and other related ICT services***

Expected Outcomes

- The Government of Eswatini together with CIIs and ICT services owners across Eswatini will keep abreast of, and fully understand the vulnerabilities, risks and levels of cyber security across CII and Information Systems in Eswatini.
- Eswatini will ensure there is resilience and availability of CIIs and ICT services across Eswatini, following the establishment and implementation of appropriate CII protection measures.
- CII and Information Systems operators have an improved capacity to manage cyber threats and incidents.
- With its comprehensive understanding of cyber threats, Eswatini will establish and implement a national and synchronized cyber incident approach.
- Eswatini will establish a centralised incident reporting and response functionality within the National Cybersecurity Agency and as a result cyber incidents are regularly and consistently reported to Eswatini's National Cybersecurity Agency.
- Through its National Cybersecurity Agency, Eswatini will be able to effectively and efficiently manage cyber incidents nationwide.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Specific Objective 1.1: Protect the critical information infrastructure and other ICT related services	1.1.1 Establish a National Critical Information Infrastructure (CII) Register	CII Register	MICT National CERT/CSIRT CII WG	By March 2021; continuous	Publication of National CII Register Frequency and number of CII identification exercises based on risk based methodologies Frequency of reviews and updates to National CII Register	MICT National CERT/CSIRT CII Operators
	1.1.2 Develop a national CII Governance	National CII Governance Framework	MICT	Published by June 2021; continually reviewed	Publication of National CII Governance Framework	MICT

	Framework which describes CII protection procedures, processes, guidelines, good practices to be adhered to by CII Operators and owners		National CERT/CSIRT CII WG		Extent of adoption and implementation of National CII Governance Framework across CII in Eswatini	National CERT/CSIRT CII Operators
	1.1.3 Establish a National Risk and Vulnerability Register and Regulations, which ensures continuous vulnerability monitoring and disclosure as well as risk assessment and management across all CIIs	Risk assessment and management Guidelines for CIIs National Risk Register National Vulnerability Register and Regulations National Vulnerability Disclosure Procedures	MICT National CERT/CSIRT CII WG	Risk assessment and management Guidelines for CIIs Published by June 2021; continually reviewed National Vulnerability Regulations and Disclosure Procedures for CIIs Published by June 2021; continually reviewed	Frequency of Risk assessment and vulnerability monitoring exercises by CIIs Frequency of update to National Risk Register Extent of adoption and implementation of National Vulnerability Regulations and Disclosure Procedures across CIIs Extent of adoption and implementation of National Risk assessment and management Guidelines across CIIs	MICT National CERT/CSIRT CII Operators

					Extent of vulnerability monitoring activities of organisations nationwide Frequency of update of vulnerability register Frequency of vulnerability disclosures	
	1.1.4 Develop and continually review CII minimum security standards and procedures to be complied with, including security audits, equipment specifications, Standard Operating Procedures (SOPs), Access Control Mechanisms, etc.	CII Minimum security standards and procedures including security audits, equipment specifications, SOPS, Access Control Mechanisms, etc.	MICT National CERT/CSIRT CII WG	Published by June 2021; continually reviewed Mandatory and Minimum cybersecurity requirements implemented across all CII by December 2021	Extent of implementation of CII Minimum security standards and procedures including security audits, equipment specifications, SOPS, Access Control Mechanisms, etc. Frequency of reviews of CII Minimum security standards and procedures including security audits, equipment specifications, SOPS, Access Control Mechanisms, etc.	MICT National CERT/CSIRT CII Operators

	1.1.5 Conduct continuous monitoring of, and regular testing of CII and Information Systems to detect vulnerabilities, illicit access, errors, etc.	Security Audits and tests to detect errors and vulnerabilities Intrusion detection system and exercises across CIIs	MICT National CERT/CSIRT CII WG	Commence by March 2021 On-going	Number and frequency of security audits and tests; Effectiveness of security audits and tests Effectiveness of intrusion detection tests/systems;	MICT National CERT/CSIRT CII Operators
Specific Objective 1.2: Manage cyber threats facing Eswatini	1.2.1 Define, publish and continuously review the minimum incident register requirements to enable dependable incident analysis against a rapidly evolving cyber landscape.	Minimum incident register requirement	MICT National CERT/CSIRT WG	Publication of Minimum incident register requirement by Jun 2021 On-going Reviews and updates	Effectiveness and reliability of the Incident reporting and analysis Extent of Incident Reporting	MICT National CERT/CSIRT
	1.2.2 Continuously identify, monitor and analyse risks and cyber threats in order to provide a real-time picture of the threats and risks facing Eswatini.	Real time picture of the state of Cybersecurity Measures to mitigate threats, risks	MICT National CERT/CSIRT WG	Commence by June 2021 On-going	Frequency of updates to overview of the state of Cybersecurity Extent of mitigation of cyber threats and risks	MICT National CERT/CSIRT

					Extent of implementation of mitigation measures	
	1.2.3 Develop and continually update a national cyber incident register for Eswatini	National cyber incident register	MICT National CERT/CSIRT WG	Published June 2021; On-going	Frequency of updates of cybersecurity incident register	MICT National CERT/CSIRT
	1.2.4 Continuously analyse cyber incidents within Eswatini and the SADC region to develop and execute measures to resolve incidents and manage cyber threats	Mitigation measures	MICT National CERT/CSIRT	On-going	Extent of implementation of mitigation measures Extent of effectiveness of measures Extent of resolution of issues/incidents	MICT National CERT/CSIRT
	1.2.5 Develop and implement national procedures for risk management and data protection	National data protection and risk management procedures	MICT National CERT/CSIRT WG	Published by June 2021; On-going review and implementation	Extent of implementation of national data protection and risk management procedures across nations	MICT National CERT/CSIRT
	1.2.6 Develop and continuously update cyber incident scenarios and cyber	Cyber incident scenarios and cyber contingency plans	MICT National CERT/CSIRT	Published by June 2021;	Extent of implementation of National Crisis Management Measures	MICT National CERT/CSIRT

	contingency plans that clearly define crisis management procedures and the roles and responsibilities of all stakeholders during cyber incidents and emergencies, and which can be used during cyber exercises	Definition of crisis management procedures and the roles and responsibilities of all stakeholder	WG	On-going review and implementation	Extent and frequency of use and/or testing of cyber incident scenarios and cyber contingency plans	
	1.2.7 Undertake regular cyber exercises to test national crisis management measures, and leverage lessons learned to improve crisis management measures and the national response to cyber incidents	Regular cyber exercises Lessons learned to improve crisis management measures and the national response to cyber incidents	MICT National CERT/CSIRT WG NCC	Commence by January 2022; On-going	Frequency of Cyber Exercises Frequency of analysis of cyber exercises to derive lessons Extent of adoption and implementation of lessons learned to improve crisis management measures and the national response to cyber incidents	MICT National CERT/CSIRT

Strategic Goal 2: Strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini

Expected Outcomes:

- Eswatini will establish a centralised and robust governance framework that has at its core, a coherent and national approach for developing, implementing and coordinating initiatives relating to cybersecurity in Eswatini.

- Eswatini will have a clear and coherent position on cybersecurity that is understood by all stakeholders and will drive the national focus in ensuring a safe, secure and resilient Cyberspace for Eswatini.
- Establish an updated and forward-looking legal and regulatory framework, which addresses on-going developments and trends in relation to cybersecurity, and includes relevant international norms that will enhance Eswatini's capability to combat cybercrime activities targeting or committed in Eswatini.
- Have a comprehensive and robust legal and regulatory framework which provides Eswatini's law enforcement and judiciary with the appropriate tools and technologies to execute their mandate with respect to cybersecurity and cybercrime Establish comprehensive and appropriate cybersecurity standards, guidelines, operational frameworks, processes, procedures applicable to Eswatini, and as a result, secure CIIs and ICT services based on well defined national cybersecurity standards.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Specific Objective 2.1: Establish a cybersecurity institutional framework to ensure the effective management of cybersecurity across Eswatini	2.1.1 Create and operationalize the National Cybersecurity Agency of Eswatini with the mandate for developing, implementing and coordinating cybersecurity initiatives in Eswatini, and provide leadership on the implementation of this strategy.	An independent and operational National Cybersecurity Agency with the mandate for developing, implementing and coordinating cybersecurity initiatives in Eswatini	MICT ESCCOM	Law by Dec. 2021 Operationalization of Agency by Dec. 2021	Promulgation of Law Extent of Operationalization of Agency	MICT ESCCOM
	2.1.2 Create the national CERT/CSIRT as a department within the National Cybersecurity Agency	An operational National CERT/CSIRT within the National Cybersecurity Agency	MICT ESCCOM NCA	Provisional National CERT/CSIRT hosted by ESCCOM by June 2021	Promulgation of Law/Regulations	MICT ESCCOM

	with clear functions and responsibilities including incident response.	with an operational Cyber Lab		Regulations by Dec 2021 Transfer of CERT/CSIRT to Agency by Dec. 2021	Extent of Operationalization of Agency	
	2.1.3 Establish a National Cybersecurity Training & Research Unit within RSTP/ UNESWA.	Operational National Cybersecurity Training & Research Unit	RSTP MICT UNESWA WG	National Cybersecurity Training & Research Unit within RSTP/UNESWA by June 2021	Extent of Operationalization Extent of delivery of cybersecurity training	RSTP MICT UNESWA
	2.1.4 Identify relevant private and public sector organisations and constitute a National Cybersecurity Council or Working Groups to provide strategic guidance to the National Cybersecurity Agency.	National Cybersecurity Council Working Groups	MICT PMO	Instrument by Dec. 2021 Committee by Dec. 2021 Working Groups for specific areas by Dec 2020	Instrument in place Extent of Operationalization of Committee and Working Groups	MICT Ministry of Justice ESCCOM Other Relevant Stakeholders Office of the Prime Minister
	2.1.5 Establish a National Cyber Defence Command Centre for Eswatini	Command Centre for Cyber Defence	Office of the Prime Minister Ministry of Defence MICT	Instrument by Dec. 2021 Operational Command Centre by Dec. 2022	Instrument in place Extent of Operationalization of Command Centre	Office of the Prime Minister Ministry of Defence

	2.1.6 Strengthen the role and mandate of law enforcement and security agencies to enhance their capacity to employ digital forensics, digital evidence and other computer enabled methods to disrupt malicious cyber activities	Strengthened mandate and role of role and mandate of law enforcement and security agencies to enhance their capacity to employ digital forensics, digital evidence and other computer enabled methods to disrupt malicious cyber activities	Ministry of Justice Office of Prime Minister REPS MICT	Instrument by Dec 2021	Instrument in place	MICT Ministry of Justice
	2.1.7 Develop a cyber defence strategy which describes the national approach for addressing cyber threats to the national security of Eswatini	National Cyber Defence Strategy	Office of the Prime Minister Ministry of Defence	National Cyber Defence Strategy – December 2021	Extent of implementation of national cyber defence strategy	Office of the Prime Minister Ministry of Defence
Specific Objective 2.3: Establish a comprehensive legal and regulatory	2.3.1 Expedite the enactment of pending	Immediate enactment of pending Legislation relating to cybersecurity	MICT Ministry of Justice	Legislation relating to cybersecurity enacted by Dec 2020	Enactment of Legislation	MICT Ministry of Justice

framework for cybersecurity	legislation relating to Cybersecurity					
	2.3.2 Undertake a gap analysis of Eswatini's Legal and Regulatory Framework in order to identify gaps related to cybersecurity. Once identified, establishing appropriate instruments to address these gaps as well as enhance Eswatini's legal and regulatory framework on cybersecurity and cybercrime.	A gap analysis report identifying gaps in current Cybersecurity Legal and Regulatory Framework Requisite instruments to address Gaps	Ministry of Justice WG MICT	Requisite instruments to address Gaps including issues relating to privacy and data protection - June. 2022	Extent of revisions to existing instruments Extent of new instruments created Enacted amendments to existing legislations or policies Enactment of new policies/legislations Extent of improvement in the effectiveness of the legal and regulatory framework or cybersecurity	Ministry of Justice MICT
	2.3.3 Subscribe to relevant regional and international instruments relating to cybersecurity and cybercrime.	International and Regional Cybersecurity and Cybercrime instruments	Ministry of Justice Ministry of Foreign Affairs MICT	On-going	Extent of implementation/domestication of the International and Regional Cybersecurity and Cybercrime Extent of improvement in the	Ministry of Justice Ministry of Foreign Affairs MICT

					effectiveness of the legal and regulatory framework for cybersecurity	
	2.3.4 Review and improve legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to enhance the fight against cybercrime	Effective legal provisions on procedural powers for investigations of cybercrime and evidentiary requirement	Ministry of Justice Law Enforcement	Legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements - June 2021; Continually reviewed	Extent of effectiveness of investigations of cybercrime Extent of disruption of cybercriminal activity as a result of improved legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements Extent of revisions made to legal provisions and evidentiary requirements	Ministry of Justice Law Enforcement
Specific Objective 2.4: Establish cybersecurity standards, guidelines, technical and operational frameworks	2.4.1 Develop and promote the adoption of a National Cybersecurity Standards Framework across CIIs and ICT services in Eswatini	National Cybersecurity Standards Framework consisting of cybersecurity standards customised or tailored for Eswatini	MICT National Cybersecurity Agency SWASA WG	Published by June 2021;	Extent of adoption/implementation of Cybersecurity Standards Framework	MICT National Cybersecurity Agency SWASA

	2.4.2 Promote the awareness and implementation of a National Cybersecurity Standards Framework across the private sector, especially the SME sector which contributes significantly to Eswatini's economy	A national programme to promote the adoption of National Cybersecurity Standards Framework across the private sector, especially among SME	National Cybersecurity Agency SWASA WG Private Sector;	Commences by June 2021; continuously after	Extent of adoption/implementation of Cybersecurity Standards Framework Number of organisations adopting and implementing the Cybersecurity Standards Framework	National Cybersecurity Agency SWASA Private Sector;

Strategic Goal 3: Build Eswatini's capacity and expertise in cybersecurity

Expected Outcomes:

- Cybersecurity becomes a core component of Eswatini's national curriculum, and taught at all levels of the education system, resulting in a sustained pool of cybersecurity professionals.
- Increased interest in cybersecurity profession by a wide range of individuals in Eswatini Cybersecurity will constitute a major component of continuous professional development programmes for all professionals.
- Organisations across Eswatini, including the National Cybersecurity Agency has the requisite technical skills and capacity to effectively manage cyber threats and cyber incidents nationally.
- Improved understanding among relevant stakeholders of the cybersecurity provisions of the legal and regulatory frameworks, consistently and effectively enforced resulting in more successful detection, investigation, and prosecution and disruption cyber criminal activities.
- Enhanced capacity and capability of Eswatini's law enforcement agencies and other relevant stakeholders to disrupt, investigate and prosecute cyber criminal activities targeting Eswatini both internally and externally.
- Increase in investment in Cybersecurity innovation and R&D in Eswatini, particularly towards the local cybersecurity service providers, resulting in year-on-year growth in the cybersecurity posture for Eswatini.
- Eswatini proactively supports national cybersecurity service providers through various measures including selective government procurement, contracts, and other incentives.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	
Specific Objective 3.1: Develop a nationwide and sustainable pool of highly skilled cybersecurity professionals	3.1.3 Develop a National Cybersecurity Education and Career Scheme aimed at promoting careers and continuous educational training in cybersecurity.	National Cybersecurity Education and Career Scheme Cybersecurity career progression strategy that promotes continuous professional education	Ministry responsible for Employment and Vocational Training; Ministry responsible Education RSTP Higher Education Institutions	Commences by March 2022;	Extent of implementation of National Cybersecurity Education and Career Scheme Extent of effectiveness of Cybersecurity career progression strategy	Ministry responsible for Employment and Vocational Training; Ministry responsible Education RSTP

			MICT		Extent of rollout of Cybersecurity career progression strategy	
	3.1.2 Review and update the current education curriculum and related materials education system in Eswatini and introduce cybersecurity aspects/concepts.	Updated school curriculum and materials	Ministry responsible for Employment and Vocational Training; Ministry responsible Education WG	Commences by June 2022; Implementation of updates is on-going activity	Extent of update of school curriculum and materials, Extent of roll-out of updated school curriculum and materials Number of graduates from school programmes with requisite cybersecurity skills Effectiveness of revisions of school curriculum and materials	Ministry responsible for Employment and Vocational Training; Ministry responsible Education
	3.1.3 Promote collaboration among universities, tertiary colleges and the private sector to create internships/studentships and work experience programs in Cybersecurity	New cybersecurity study and work experience programs	Ministry responsible for Employment and Vocational Training; Ministry responsible Education Academia Private Sector	Commences by June 2022 Implementation is on-going activity	Number of new cybersecurity study and work experience programs Number of graduates from new cybersecurity study and work experience programs	Ministry responsible for Employment and Vocational Training; Ministry responsible Education Academia Private Sector

	3.1.4 Define minimum standards in cybersecurity training and education qualifications in Eswatini	Minimum standards in cybersecurity training and education	Ministry responsible for Education National Cybersecurity Agency	Commences by Mar 2022 Implementation is on-going activity	Extent of implementation in/compliance with mandatory and minimum standards in cybersecurity training and education	Ministry responsible Education
Specific Objective 3.2: Build technical skills and capacity in cyber resilience and incident response	3.2.1 Assess the capacity and expertise of the National Cybersecurity Agency and other relevant public institutions to identify and address gaps/weaknesses in cybersecurity skills	Evaluation of the capacity and expertise of the National Cybersecurity Agency and other relevant public institutions Measures to address gaps/weaknesses in cybersecurity skills in the National Cybersecurity Agency and other relevant public institutions	ESCCOM/MICT National Cybersecurity Agency	Commences by March 2022 On-going activity	Extent of implementation of measures addressing gaps and weaknesses Frequency/Effectiveness of Evaluations of capacity and technical expertise Effectiveness of measures addressing gaps and weaknesses	ESCCOM/MICT National Cybersecurity Agency
	3.2.2 Train and educate CERT/CSIRT Staff and other relevant government institutions to develop their skills and capacity to manage cyber threats and cyber incidents	Capacity building and training programme to build skills and capacity in national cyber incident preparedness, response and recovery activities	ESCCOM/MICT National Cybersecurity Agency	Commence by June 2021	Extent of Implementation of Capacity building and Training Programme Effectiveness of Capacity building and Training Programme Number of incidents/attacks/thre	ESCCOM/MICT National Cybersecurity Agency

	effectively, particularly national cyber incident preparedness, response and recovery activities				ats/risks prevented/mitigated as a direct consequence of training programme	
Specific Objective 3.3: Build the technical skills and capacity required to investigate and prosecute cybercrimes, and effectively enforce established cybersecurity legal and regulatory instruments in Eswatini	3.3.1 Continuously train and educate law enforcement agencies and the judiciary to develop and enhance their capacity and capability to enforce the cybersecurity related provisions of the legal and regulatory framework, including investigation and prosecution of cybercrimes.	National Cybersecurity Training Programme for Law Enforcement and Judiciary	MICT Min of Justice Royal Eswatini Police Service	Commences by June 2021; Continuous	Extent of Implementation of National Cybersecurity Training Programme for Law Enforcement and Judiciary Effectiveness of Training Programme Frequency of Trainings Number of incidents/attacks/threats/risks prevented/mitigated as a direct consequence of training programme	MICT Min of Justice Royal Eswatini Police Service
	3.3.2 Conduct digital forensics and evidence handling	Digital forensics and evidence handling courses	MICT Min of Justice	Commences by June 2021	Frequency of digital forensics and evidence handling courses	MICT Min of Justice

	courses for all relevant agencies involved to enhance detection, investigation and prosecution of cybercrimes.		Royal Eswatini Police Service All relevant agencies		Effectiveness of digital forensics and evidence handling courses Number of incidents/attacks/threats/risks prevented/mitigated as a direct consequence of digital forensics and evidence handling courses	Royal Eswatini Police Service All relevant agencies
Specific Objective 3.4: Foster Innovation and Research & Development (R&D) in cybersecurity	3.4.1 Promote and support cybersecurity competitions and R&D projects in Universities, Colleges and Schools	Funding and incentive programmes for Universities engaged in Cybersecurity R & D Competitions in schools on cybersecurity	Academia; Ministry of Education; Private Sector WG	Commences by Dec 2022	Number of universities participating in funding and incentive programme Number of cybersecurity competitions	Academia; Ministry of Education; Private Sector
	3.4.2 Establish national funding and incentive programmes to support national enterprises providing Cybersecurity solutions	Funding and incentive programmes for national enterprises providing Cybersecurity solutions	Ministry responsible for public contracts and procurement Ministry of Finance Private Sector	Commences by Dec 2022	Number of Enterprises participating in funding and incentive programme	Ministry for public contracts and procurement Ministry of Finance Private Sector

					Effectiveness of Funding and incentive programmes Extent of Implementation of National Investment Incentive Programme	
	3.4.3 Establish partnerships between education sector, public and private sector, and international partners to enable Eswatini individuals and organisations to take part in national and international cybersecurity capacity building and R&D activities.	Partnerships to support participation of Eswatini individuals and organisations in national and international cybersecurity capacity building and R&D activities	Ministry of ICT National Cybersecurity Agency RSTP Private Sector Institutions of Higher Learning	Commences by Dec 2022	Extent of participation of Eswatini individuals and organisations in national and international cybersecurity capacity building and R&D activities; Number of partnerships created which support participation of organizations and individuals in national and international cybersecurity capacity building and R&D activities	Ministry of ICT National Cybersecurity Agency RSTP Private Sector International Development Agency

Strategic Goal 4: Foster a safe and secure information society for Eswatini
Expected Outcomes

- Cybersecurity good practices are widely established both in private and public sectors across Eswatini, resulting in continuous reduction in the number of seriousness and high-impact cyber-attacks in Eswatini.
- Organisations and individuals in Eswatini, especially high ranking government officials, legislators, private sector board members and management, understand the need for cybersecurity, responsibilities, liabilities, together with the measures for protecting their organisations establishment of a cybersecurity culture in Eswatini.
- Eswatini's e-government services are underpinned by cybersecurity requirements, baselines and functionality, and as a result are trusted and used with confidence by organisations and individuals in Eswatini.
- Robust and secure e-Government services deployed across Eswatini. Deploy security measures to address comprehensively concerns expressed by users of e-government services and disseminate widely information gathered on how these concerns have been addressed.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Specific Objective 4.1: Establish a cybersecurity mindset and culture in Eswatini	4.1.1 Conduct a national study to assess levels of Cybersecurity awareness across Eswatini. Then develop and roll-out tailored national awareness programmes targeting all groups of users, especially those who are vulnerable and at risk such as children, women, seniors citizens and other vulnerable groups	Nationwide study of the levels of awareness of cybersecurity across Eswatini National awareness programmes targeting all groups of users, especially those who are vulnerable and at risk such as children, women and other vulnerable groups. Child Online Protection Programme	MICT Ministry responsible for Welfare and Social Affairs Civil Society; National Cybersecurity Agency	Starts by Mar 2021; Continuous	Level of awareness Number/frequency of cybersecurity campaigns Effectiveness of campaigns Extent and frequency of assessment of national levels of cybersecurity awareness Robustness of assessment findings	MICT Ministry responsible for welfare and Social Affairs International Partners Civil Society Universal access fund Private Sector

	4.1.2 Publicise cybersecurity good practices nationwide to instil a cybersecurity culture across Eswatini	National cybersecurity culture roadmap for instilling a cybersecurity mind-set and culture Widespread dissemination of cyber security good practices across multiple channels of communication	Civil Society; National Cybersecurity Agency Private Sector WG	Starts by Mar 2021;	Extent of implementation of National roadmap Frequency of Publication/Dissemination of cyber security good practices across multiple channels of communication such as churches, media, sign boards, etc.	Civil Society; National Cybersecurity Agency Private Sector;
	4.1.3 Conduct mandatory cybersecurity training of high ranking government officials, legislators, private sector board members and management	Mandatory Cybersecurity Training Programmes for high ranking government officials, legislators, private sector board members and management	RSTP National Cybersecurity Agency Private Sector MICT ESIMPA	Starts by Mar 2022;	Extent of cybersecurity knowledge possessed by high ranking government officials, legislators, private sector board members and management taking part in trainings Effectiveness of mandatory cybersecurity training of high ranking government officials, legislators, private sector board members and management	RSTP National Cybersecurity Agency Private Sector;

					Frequency of mandatory high ranking government officials, legislators, private sector board members and management	
Specific Objective 4.2: Create a secure environment for e-government services in Eswatini	4.2.1 Deploy PKI across the nation especially in e-government services so as to leverage the security features of PKI relating to confidentiality, authentication and data integrity	PKI implementation plan	MICT E-government Unit	Starts by Sept 2021;	No. of e-government services incorporating PKI	MICT
	4.2.2 Encourage the transition from IPV4 to IPV6 protocol to leverage the IPV6 security features relating to confidentiality, integrity and authenticity of information data	IPV4 to IPV6 Implementation Plan	MICT Network Operators ISPs RSTP	Starts by Dec 2021;	Extent of implementation of IPV4 to IPV6 Transition	MICT
	4.2.3 Ensure mandatory or	Mandatory minimum-security requirements	MICT	Starts by Mar 2021;	Extent of implementation/compl	MICT

	minimum security requirements are considered during the development of e-government services	for development of e-government services.	National Cybersecurity Agency Private sector E-Government Unit		iance of mandatory minimum-security requirements by e-government services.	National Cybersecurity Agency Private sector All relevant stakeholders
Specific Objective 4.3: Build trust in the use of e-government services	4.3.1 Establish Points of Contact within the National Cybersecurity Agency who will interface with individuals and organisations across Eswatini to collect information on their security concerns with e-government services, and analyse how these concerns have been addressed or resolved	Points of Contact responsible for collecting information on security concerns with e-government services Measures to address security concerns with e-government services	National Cybersecurity Agency MICT E-Gov Unit	Starts by Dec 2021 On-going activity	Extent of collection and analysis of information on the security concerns on e-government services Extent of implementation of measures addressing security concerns on e-government services Extent of trust in e-government and e-commerce services fostered in individuals and organisation	National Cybersecurity Agency
	4.3.2 Publicise widely and regularly across Eswatini how e-government services have been secured to build trust in the use e-government services	Dissemination of information on how e-government services have been secured	National Cybersecurity Agency MICT E-Gov Unit Relevant departments	Starts by Dec 2021 On-going activity	Effectiveness of Dissemination of information on how e-government services have been secured Frequency of Dissemination of information on how e-	Starts by Dec 2021 On-going activity

	and Eswatini's cyberspace in general				government services have been secured	

Strategic Goal 5: Strengthen cooperation, collaboration and partnerships on cybersecurity

Expected Outcomes

- Eswatini has more effective information sharing on cybersecurity issues both locally and internationally, which in effect translate to more effective management of cyber threats nationally.
- Effective collaboration with all relevant stakeholders on cybersecurity issues, and active participation in international cybersecurity activities, resulting in improved management of cyber threats and disruption of cyber criminal activity targeting and/or originating from Eswatini.

Specific Objectives	Strategies/ Actions	Deliverables/ Outputs	Lead Implementing Agency and Support	Time Frame	Key Performance Indicators	Possible Funding Sources and Mechanisms
Specific Objective 5.1: Promote collaboration and information sharing on cybersecurity	5.1.1 Establish a network of sectorial cybersecurity focal points together with an information sharing framework to enhance collaboration and mutual exchange of information on Cybersecurity locally and internationally	Information Sharing and Collaboration Framework Network of sectorial cybersecurity focal points	MICT National Cybersecurity Agency WG	Network established by June 2021	Extent and frequency of information sharing Effectiveness of information sharing Extent of mitigation of cyber threats/incidents/vulnerabilities/incidents as a result of information sharing	MICT National Cybersecurity Agency
	5.1.2 Mandate the National Cybersecurity Agency as the central body for overseeing information sharing	National Cybersecurity Agency is the national body for overseeing information sharing and collaboration on cyber security	MICTESCCOM	Commences in Dec 2020where MICT will act as national body till operational National Agency	Extent and frequency of information sharing Effectiveness of information sharing Extent of mitigation of cyber	MICT ESCCOM

	and collaboration on cyber security.	Enhanced information sharing mechanism/frameworks		On-going activity	threats/incidents/vulnerabilities/incidents as a result of information sharing	
	5.1.3 Create a national fora to promote a national information sharing on cybersecurity	National Fora for national information sharing	MICT National Cybersecurity Agency	Commence by June 2021	Extent of participation of local stakeholders in national discussions/ fora on cybersecurity Extent and frequency of information sharing at national fora Effectiveness of information sharing resulting from national fora Extent of mitigation of cyber threats/incidents/vulnerabilities/incidents as a result of information sharing information sharing at national fora	MICT National Cybersecurity Agency
Specific Objective 5.2: Establish partnerships to promote collaboration and cooperation in addressing	5.2.1 Develop an International Collaboration Strategy that outlines how international collaboration on	International collaboration management Strategy for Cybersecurity Improved international	MICT National Cybersecurity Agency REPS	June 2022	Effectiveness and efficiency in international collaboration Extent of implementation of International	MICT National Cybersecurity Agency

cybersecurity issues locally and internationally	cybersecurity and cybercrime is managed	collaboration and cooperation on cybersecurity National Budget for more active collaboration and cooperation on international and regional activities on cybersecurity and cybercrime	Min of Justice Ministry of Foreign Affairs		collaboration management Strategy for Cybersecurity Extent of implementation of National Budget for more active collaboration and cooperation on international and regional activities on cybersecurity and cybercrime Number of beneficiaries of Funding streams to support collaboration and cooperation on international and regional activities on cybersecurity and cybercrime Frequency/Effectiveness of findings/lessons resulting from collaboration and cooperation on international and regional activities on cybersecurity and cybercrime	Ministry of Foreign Affairs
	5.2.2 Enhance partnerships with local partners, other states and international stakeholders to collaboratively address cyber security	Cooperation & collaboration agreements with identified bodies and nations Signatory to international accords	MICT National Cybersecurity Agency Ministry of Foreign Affairs	Commence by June 2022	Number of agreements signed and implemented and effective exchange and use of information Number of cyber threats identified and mitigated as a direct result of international cooperation & collaboration	MICT National Cybersecurity Agency Ministry of Foreign Affairs

	and combat cybercrimes				agreements, and international accords Extent of implementation of international cooperation & collaboration agreements, and international accords Extent of international cooperation coordination and collaboration as a result of international cooperation & collaboration agreements, and international accords	
	Subscribe to and participate in all relevant regional and international discussions/ fora on cybersecurity	More active participation in, and collaboration on relevant regional and international discussions/ fora on cybersecurity	MICT National Cybersecurity Agency Ministry of Foreign Affairs	Commence by June 2020	Extent of participation in, and collaboration on relevant regional and international discussions/ fora on cybersecurity Number of regional and international discussions/ fora on cybersecurity where participation/collaboration occurred	MICT National Cybersecurity Agency Ministry of Foreign Affairs

APPENDIX B – STRATEGY QUICK WIN PROJECTS

Strategic Goal 1: Enhance the security and resilience of national critical information infrastructure and other related ICT systems
• 1.1.1 Establish a National Critical Information Infrastructure Register • 1.1.2 Develop a national CII Governance Framework which describes CII protection procedures, processes, guidelines, good practices to be adhered to by CII Operators and owners • 1.1.3 Establish a National Risk and Vulnerability Register and Regulations, which ensures continuous vulnerability monitoring and disclosure as well as risk assessment and management across all CIIs • 1.1.4 Develop and continually review CII minimum security standards and procedures to be complied with, including security audits, equipment specifications, Standard Operating Procedures (SOPs), Access Control Mechanisms, etc. • 1.2.3 Develop and continually update a national cyber incident register for Eswatini
Strategic Goal 2: Strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini
• 2.1.1 Create and operationalize the National Cybersecurity Agency of Eswatini with the mandate for developing, implementing and coordinating cybersecurity initiatives in Eswatini, and provide leadership on the implementation of this strategy • 2.1.2 Create the national CERT/CSIRT as a department within the National Cybersecurity Agency with clear functions and responsibilities including incident response • 2.1.3 Establish Working Groups for specific areas of Cybersecurity • 2.1.4 establish the National Cybersecurity Council for Eswatini • 2.1.5 Expedite the enactment of pending legislation relating to Cybersecurity • 2.1.6 Undertake a gap analysis of Eswatini's Legal and Regulatory Framework in order to identify gaps related to cybersecurity. Once identified, establishing appropriate instruments to address these gaps as well as enhance Eswatini's legal and regulatory framework on cybersecurity and cybercrime • 2.1.7 Develop and promote the adoption of a National Cybersecurity Standards Framework across CIIs and ICT services in Eswatini
Strategic Goal 3: Build Eswatini's capacity and expertise in cybersecurity
• 3.1.1 Develop a National Cybersecurity Education and Career Scheme aimed at promoting careers and continuous educational training in cybersecurity • 3.1.2 Review and update the current education curriculum and related materials education system in Eswatini and introduce cybersecurity aspects/concepts

- 3.2.1 Assess the capacity and expertise of the National Cybersecurity Agency and other relevant government institutions to identify and address gaps/weaknesses in skills
- 3.3.1 Continuously train and educate law enforcement agencies and the judiciary to develop and enhance their capacity and capability to enforce the cybersecurity related provisions of the legal and regulatory framework, including investigation and prosecution of cybercrimes
- 3.4.2 Establish a national funding and incentive programme to support national enterprises providing Cybersecurity solutions

Strategic Goal 4: Foster a safe and secure information society for Eswatini

- 4.1.1 Conduct a national study to assess levels of Cybersecurity awareness across Eswatini. Then develop and roll-out tailored national awareness programmes targeting all groups of users, especially those who are vulnerable and at risk such as children, women, seniors citizens and other vulnerable groups
- 4.1.2 Publicize cybersecurity good practices nationwide to institute a cybersecurity culture across Eswatini.
- 4.1.3 Conduct cybersecurity training of high ranking government officials, legislators, private sector board members and management
- 4.2.3 Ensure mandatory and minimum security requirements are considered during the development of e-government and e-commerce services

Strategic Goal 5: Promote collaboration and information sharing on cybersecurity

- 5.1.1 Establish a network of sectorial cybersecurity focal points together with an information sharing framework to enhance collaboration and mutual exchange of information on Cybersecurity locally and internationally
- 5.2.1 Develop an International Collaboration Strategy that outlines how international collaboration on cybersecurity and cybercrime is managed and funded

APPENDIX C – GLOSSARY

Authentication:	The process of verifying the identity or other attributes of a user, process or device.
Big data:	Data sets, which are too large or complex to process and manage with traditional software tools in a timely way, and require custom-built processing capabilities to manage.
Bitcoin:	A digital currency and payment system.
Cryptography:	The practice and study of techniques for secure communication which include the analysing and deciphering codes and ciphers.
Cyber-attack:	Deliberate action to exploit computer systems and networks to cause harm.
Cybercrime:	Crimes that can only be committed through the use of ICT devices where the devices are both the tool for the crime and target of the crime and traditional crimes which can be increased in scale and reach by the use of computers, computer networks or any other forms of ICTs.
Cyber ecosystem:	The entirety of interconnected data, individuals, infrastructure, processes, data, ICTs, together with the environment and conditions that affect these interdependencies.
Cyber incident:	An event that really or potentially poses a threat to an internet-connected device, a computer, or network and/or the data processed, stored, or transmitted on these systems, and which may require a response action to mitigate the consequences.
Cyber resilience:	The general ability of systems, networks and organisations to withstand cyber incidents and recover from harm wherever caused.
Cyber security:	The protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cyberspace:	The interdependent network of IT infrastructures including internet connected devices, computer systems, telecommunications networks, and the Internet
Cyber threat:	Anything capable of compromising the security of, or causing harm to, internet-connected device, computer, software or network, data on them, the services they provide or under pin.
Distributed Denial of Service (DDoS):	A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet; this sort of attack is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled
E-commerce:	Commerce conducted, or facilitated by, the Internet.

Incident management:	Management and coordination of activities to examine and rectify a current or potential occurrence of an adverse cyber incident that may compromise a system or network.
Incident response:	Activities that address short term and direct effects or cyber incidents and support short term recovery
Industrial Internet of Things (IIoT)	The use of Internet of Things technologies in manufacturing and industry.
Insider:	Someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.
Integrity:	The property that information has not been changed accidentally, or deliberately, and is accurate and complete.
Internet:	A global computer network consisting of interconnected networks using standardised protocols and providing a variety of information and communication facilities
Internet of Things:	The entirety of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.
Malware:	Malicious software or code; includes viruses, worms, Trojans and spyware.
Patching:	Patching is the process of updating software to fix bugs and vulnerabilities.
Penetration testing:	Activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.
Phishing:	The use of emails that appear to originate from a trusted source, to deceive recipients into clicking on malicious links or attachments that are loaded with malware, or share sensitive information with an unauthorised third party.
Ransomware:	Malicious software that denies the user access to their files, computer or device until a ransom is paid.
Risk:	The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.
Security by design:	Refers to the concept where software, hardware and systems that have been designed from the ground up to be secure.
Social engineering:	Refers to the methods employed by malicious cyber attackers to deceive and manipulate victims into performing an action or divulging confidential information.
Virus:	Malicious software that can spread to other files.
Vulnerability:	Bugs in software programs that have the potential to be exploited by malicious cyber attackers.

APPENDIX D – ACRONYMS

CERT/CIRT/CSIRT	Computer Emergency Response Team/ Computer Incident Response Team/Computer Security Incident Response Team (can be used interchangeably)
CII	Critical Information Infrastructure
DPMO	Deputy Prime Minister's Office
E-Gov Unit	Electronic Government Unit
ESCCOM	Eswatini Communications Commission (communications regulator)
ICT	Information and Communications Technology
ISPs	Internet Service Providers
MICT	Ministry of Information, Communications and Technology
MoD	Ministry of Defence
MoET	Ministry of Education and Training
MoF	Ministry of Finance
MoFAIC	Ministry of Foreign Affairs and International Cooperation
MoJCA	Ministry of Justice and Constitutional Affairs
NCA	National Cybersecurity Agency (a unit within ESCCOM)
NCC	National Cybersecurity Council
NCS	National Cybersecurity Strategy
PMO/OPM	Prime Minister's Office/ Office of the Prime Minister
REPS	Royal Eswatini Police Service
RSTP/RETP	Royal Eswatini Technology Park
SME	Small and Medium sized Enterprise
SWASA/ESWASA	Eswatini Standards Authority
UEDF	Umbutfo Eswatini Defence Force
UNESWA	University of Eswatini
WG	Working Group (technical groups formed for specific aspects of security)