

INTERNATIONAL COOPERATION

tourist convenience

curriculum REFORM

Republic of Mauritius

GOVERNMENT PROCESS DEVELOPMENT TRAINING
NATIONAL ICT STRATEGIC PLAN

2007-2011

MEASURING THE INFORMATION ECONOMY
Broadband

emerging technologies, applications and standards

ELECTRONIC COMMUNICATIONS infrastructure

SECTORAL eGovernance

EVENT HOSTING

ict for social development

EXPLOITATION OF ICT

in the GDP HORIZONTAL TRANSFER

BUSINESS PROCESS OUTSOURCING TRAINING

information SECURITY

ICT EXPORTS

ICT Manpower

policy, regulatory and institutional framework

Development and Planning

public internet access points

local content

...now Scaling Up

ICT DOMESTIC

TECHNOLOGY TEST BED

ICT REGIONAL HUB

Multi-channel services



PART THREE

ANNEXURE I : National Information Security Strategy

The National Information Security Strategy Plan (NISSP) is an important part of the Government's information society policy. Its main purpose will be to combat threats to information security. The NISSP will provide a common platform for the information security efforts of the Government, businesses, Organisations and individual citizens.

Information Security Concerns

The Information Society

Today's information society is epitomised by everyone now being able to send and receive vast quantities of information quickly, over great distances and at a low cost. At the same time, almost everyone can also access an infinite amount of information, knowledge and facts in a rapid manner. Rapid escalation in the level of e-business deployment leads to a multitude of electronic services currently available on the market today – and so far we have only scraped the tip of the iceberg in terms of developments within this area. The deployment of information technology has permeated almost every activity within society.

The risks are increasing in scope

Ubiquitous use of information technology has made society vulnerable within a variety of new areas. Malicious attacks on information systems can cause serious damage and disruption in normal services, e.g. in the form of unauthorised access, virus spreading and denial of service. Attacks can be mounted at any time, against anyone and from anywhere. In other words, society is facing completely new security challenges, the gravest of them being identifiable states' or factions' capabilities to organise and launch co-ordinated IT attacks with the intention of paralysing critical functions in a society. Beyond deliberate malicious attacks, vulnerability can also be attributable to inadvertent incidents – resulting from sheer carelessness or user ignorance. Vulnerability can also be increased by extreme weather conditions, such as floods and thunder storms, which also can have an effect on the scope of risk. Instability in information systems can also undermine confidence and thus inhibit widespread use of IT as a tool for creating new business opportunities.

Key challenges facing the information society

Identification of Critical Information Infrastructures

Information infrastructures can be described as critical if functionality of society, enterprises or individuals is severely affected by such a system's failure. It is imperative to identify these systems and gauge their position on a criticality scale. This is a prerequisite for risk assessments and implementation of critical protective measures. One distinct challenge here will involve identifying and securing infrastructures that are critical for the functioning of the society as a whole.

Securing critical IT infrastructures

Enterprises' security measures should be scaled according to an assessment of the identified risks. However, the challenge here will be to define a comprehensive set of generic criteria for securing critical functions in the society, partly because they differ so greatly. A generic set of common security measures will take care of the basic protection. Then, additional security measures at national, regional and local level can be implemented in particularly high-risk

situations. Security should include measures on physical, logical, and administrative levels. The development of suitable codes of best practice / standards in this area will undoubtedly pose a challenge.

Secure e-transactions

Far more extensive use of cryptography is recommended if in order to strengthen trust and confidence in electronic communication, e.g. to ensure that financial transactions are indeed secure and that private communications remain private. However, there is a potential drawback to private individuals or enterprises using advanced cryptography to protect their own information against unauthorised access, as this could obstruct police investigations into serious crime and cyber terrorism. These considerations must be weighed carefully against each other.

Drawing up regulations

National legislation, regulations and guidelines on information security have been developed over time and are based on a variety of needs. Many enterprises are obliged to follow several different types of regulations when they process many different kinds of information. It is therefore important to ensure that relevant regulations accommodate various security needs and take privacy into sufficient consideration. Development of new, and amendment of already existing, regulations shall be done in such a way as to make enforcement as easy and straightforward as possible.

Enterprises' focus on security

The management is primarily responsible for assuring an enterprise's assets, whether on behalf of society or the enterprise itself. The employees must be made aware of the substantial financial damage that could occur if there is a security breach. Large and middle-sized companies need to set up an in-house IT-security unit / task force with clearly defined responsibilities. The management ought to allocate adequate resources for security work. The companies without an in-house security unit / task force must see to it that the company commands enough skills to be able to assure adequate IT-security by engaging the services of external security experts. Security consequences of outsourcing of IT services need also to be evaluated. Clear lines of responsibility must exist for those implementing the IT-security measures and those auditing the actual implementation.

Emerging Security Risks

Increasing use of laptops, mobile phones and PDAs with Internet access are bringing new risks for businesses. Broadband technology enables IT equipment to stay "always on". Exchanging and synchronising data between portable and stationary units is becoming easier all the time. All this creates new challenges connected with uncontrolled information exchange and results in increased vulnerability and exposure to potential new types of attack.

A culture of security in society

We need to establish a culture of security in enterprises, public sector and the citizens, linked to the use of IT. A lot of users are not aware of the risks arising from using an information network. Many do not know of existing solutions for avoiding potential threats. This makes it difficult for an individual to assess the risks associated with Internet access. This also indicates a need to raise users' awareness of security threats and improve their skills in dealing with them. Safe use of the Internet has also an ethical dimension. This exacts new demands on acceptable ethical codes of conduct both on the part of Internet service providers and users themselves.

2. Principles of the National Information Security Strategy

The World Summit on Information Society Geneva Declaration of Principles states “strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs”. It further states that a “... global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies”.

The WSIS Action Line C5 recommends that member states implement measures along the following areas for Information Security:-

- Critical information infrastructure protection;
- Promotion of a global culture of cybersecurity;
- Harmonising national legal approaches, international legal coordination & enforcement;
- Countering spam;
- Developing watch, warning and incident response capabilities;
- Information sharing of national approaches, good practices and guidelines;
- Privacy, data and consumer protection.

The National Information Security Strategy is thus based on the WSIS Action Line C5 of the Geneva Declaration.

National Information Security Vision and Objectives

The National Information Security Strategy (NISS) is an important part of the Government’s ICT policy.

The vision for Information Security is aligned with the ICT vision is to “Transform Mauritius into an information-secure society, which supports the development of a trustworthy and competitive information economy”

The NISS will provide a common platform for the information security efforts of the Government, businesses, Organisations and individual citizens. The main goal of the NISS is to build trust and security in the use of ICTs.

The main objectives of the NISS are to:-

- Streamline and improve co-ordination on the implementation of information security measures at the national and international level;
- Protect critical information infrastructure from disruption through security breaches;
- Promote information security risk management and adoption of Information Security Standards at national level;
- Establish a framework for implementation of information assurance in critical sectors of the economy such as public utilities, telecommunications, transport, tourism, financial services, public sector, manufacturing and agriculture and developing a framework for managing information security risks at the national level;
- Establish an institutional framework that will be responsible for the monitoring of the information security situation at the national level, dissemination of advisories on latest information security alerts and management of information security risks at the national level including the reporting of information security breaches and incidents;
- Promote secure e-commerce and e-government services;
- Safeguard the privacy rights of individuals when using electronic communications and
- Improving awareness and competence in information security and sharing of best practices at the national level through the development of a culture of cyber security at national level.

National Information Security Strategy Measures

The measures of the NISS are based around the following areas of focus:-

- A. Information Security co-operation at national and international level
- B. Information Security Awareness and Education
- C. Trust and Confidentiality
- D. Information Security Risk Management
- E. Internet Governance
- F. Information Assurance

Information Security Cooperation at national and international level

The purpose of the National Information Security Strategy is to influence the creation of standards, policy guidelines and cooperation for promoting information security and to ensure that the division of responsibilities between the various actors in the field of information security is clear.

To this effect, it is proposed that a National Information Security Committee be set up under the aegis of the Ministry of IT and Telecommunications, including representatives from NCB, ICT Authority, operators of critical information infrastructure and regulatory bodies of other sectors to monitor the implementation of the measures of this Strategy, review and make proposals to update each regulatory authority's legislation impacting Information Security, propose clear cut guidelines for Information Security implementation in private sector and make proposals to Government for updating the Strategy after three to four years.

A working group will be set up reporting to the National Information Security Committee to provide status on information security and business continuity preparedness and national risk profiling on a regular basis. Operators of critical information infrastructure would also be represented in the working group. Closer collaboration with countries enjoying a more advanced culture of security will also be considered.

Information Security Awareness and Education

In a secure information society, everyone must be aware of the information security risks of their actions and of their responsibility in preventing these risks. The National Information Security Strategy is intended to raise the level of competence by investing in the expertise of information security professionals on one hand and in the general awareness of information security of all actors on the other.

All participants shall be made aware of potential threats, options, limitations and necessary action to advance establishment of a culture of IT security. The Government will promote awareness in this respect. All individuals are, however, responsible for obtaining necessary knowledge themselves, and to ensure compliance with the relevant legislation. Failure to gain essential knowledge could be detrimental to others, for which one could be held legally liable.

The following measures are proposed to this effect:-

- o Implement a National Information Security Awareness campaign targeting people in the workplace, public sector, students and general public to increase the awareness of individuals regarding information security issues by distributing factual information, producing info spots and incorporating information security education at all school levels. Distribute best practices for raising awareness to all educational institutions.
- o Review of curriculum for Computer Science and related subjects at Tertiary Level to include relevant information pertaining to needs of industry and businesses with regards to information security;

- Devise means for increasing number of professionals with Information Security Professional Qualifications (such as CISSP, CISA amongst others)
- Top management in private companies and public sector organisations are responsible to ensure their organisation have the necessary skills within Information Security based on well defined needs, and the organisation is committed to skills-promoting measures for its employees on Information Security.
- Suppliers of IT systems shall aim at transparency in informing customers with the level of security that their product can guarantee, under given circumstances. Suppliers should also follow internationally recognised security standards and provide support to users in the event of fault situations. Service Providers who place IT equipments and systems at the disposal of others should follow internationally recognised benchmarked security standards, defining security attributes as well as clarifying responsibilities held by the equipment's owner and its users
- Promote setting up of internationally recognised Information Security Association and local chapters of Internationally recognised bodies in the field
- Promote cooperation between industry and academia on knowledge sharing in information security areas through the holding of regular annual conferences on Information Security targeting major players and participants in the region.

Trust and Confidentiality

Building an information society with information security cannot happen at the expense of the fundamental rights and liberties of individuals and other actors. In a secure information society, all actors must be able to trust that their information and messages are processed and stored with confidentiality and will not be disclosed to unauthorised parties. Furthermore, everyone must have easy access to information for which they have authorisation.

To this end, the following measures will be implemented:

- The provisions under the Data Protection Act shall be implemented.
- Ensure that freedom of speech, confidentiality of communications, protection of privacy and other fundamental rights are taken into account in the legislation, official instructions and standards relating to information society services, electronic communications and information security, and in e-transactions services provided by public authorities;
- Establish a consultative process towards building a National Cryptography Policy;
- Implement appropriate mechanisms for the setting up of a Mauritian Public Key Infrastructure (PKI), including Controller of Certification Authority (CCA) for certifying local Certificate Authorities (CA). A Government PKI will be set up for the implementation of secure e-government services.

Information Security Risk Management

There is a need to provide greater transparency on how information security is handled in Organisations to improve trust and give comfort to users. In addition, monitoring of compliance to information security controls is done mainly at the level of the large organisations and Information Security standards has been adopted by the public and some large organisations mainly.

In Mauritius, there is no institution performing the role of a Computer Emergency Response Team (CERT) as is the case in other countries such as US, UK, India and Australia amongst others. To fight the increasing incidents of cybercrime, a vast majority of countries around the world have set up their own CERTs. The role of a CERT is to work with the Internet community to facilitate response to computer security incidents, to take proactive steps to raise the

community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. Moreover, in case of national disaster, the leadership responsible for measures related to preparedness and recovery for the national economy is not clear.

The following measures are proposed:-

- Set up a Mauritian CERT, (CERT-MU) for monitoring the national situation in information security risks, and constantly updated to provide timely information on the national situation to the major stakeholders CERT-MU will also be involved in activities such as Critical Information Infrastructure Protection and performing information security risk profiling and convey information on them and required counter-measures to all stakeholders. CERT-MU will be represented in the National Information Security Committee as well to provide status on the information security preparedness at national level.;
- A common set of criteria will be created to facilitate identification of critical IT infrastructures and systems. A method will be devised for risk and vulnerability assessments. The sectors will outline quality assurance standards for confidentiality, integrity and availability. The government will stimulate the development of security models, tools and mechanisms for risk analysis in order to encourage more efficient and user-friendly handling of IT security implementation.
- Security categorisation of information and security standards for private companies information processing should be adopted as far as possible.
- Information Security standards will be implemented in the Civil Service and parastatal organisations.
- Set up a working group responsible for identifying and monitoring critical information infrastructure protection under the National Information Security Committee.
- Set up a framework for monitoring Internet traffic which might be harmful to the nation and society;
- Promote the adoption and compliance to Information Security standards across the critical sectors of the society including SMEs.

Internet Governance

The main components under the WSIS Action Line C5 for Security issues of Internet Governance pertain to the problem of spamming, new forms of cyber crimes such as phishing, and safety of children online.

The measures to this effect are as follows:-

- Implement the recommendations of the Anti-Spam Action Plan;
- Enact appropriate legislations to counter the problem of spamming, new forms of cybercrimes such as phishing and to protect children online.
- Develop a Child Safety Action Plan, which will provide a roadmap for the protection of children and consumers online.

Information Assurance

Current status shows that, in few sectors, there is a reasonable number of documented policies and processes on information security. However there is a noticeable lack of monitoring of its compliance. In sectors, like, banking and financial sector, where there is a regime of strict and mandatory compliance, assurance activities on Information Security compliances are carried as per the requirement.

There is a unanimous concern that mandatory compliance and assurance processes would be a harsh financial burden on SMEs or small organisations. International Information Security standards could be tailored to reduce this

burden. Moreover, in the initial stages, only critical sector organisations be targeted for a mandatory Information Assurance which would subsequently widened to all organisations after a specific timeframe.

Thus the broad objectives of this area of focus would be to:

- a. Ensure that procedures and information security controls in place and are complied with.
- b. Provide a high degree of confidence the appropriate security controls are being effectively put in place for critical information infrastructure, which would minimise any disruptions in case of security breaches.

It is proposed to adopt the National Information Security Assurance Framework similar to the one implemented in India. To meet the above objectives, the following measures will be implemented:

- Promote the adoption of Information Security Standards at the National Level.
- Develop and implement a National Information Security Assurance Program (NISAP) for the public sector and for Organisation operation Critical Information Infrastructure. The salient features of this programme will be as follows:-
 - Government and critical infrastructure organisations (public or private) must have a security policy and nominate a point of contact;
 - Mandatory requirement for organisations to implement security controls and report security incidents to CERT-MU;
 - CERT-MU will create and maintain a panel of auditors of IT security, including penetrations testing and vulnerability assessment;
 - All organisations must be subject to third party audit from the panel once a year and whenever major configurations change; and
 - Security compliance to be reported to CERT-MU on a periodic basis

11. List of Abbreviations

AHRIM	Association hôteliers et restaurateurs de L'île Maurice
ASMH	Association of Small and Medium sized Hotels
BOI	Board of Investment Mauritius
BPML	Business Parks of Mauritius Ltd
BPO	Business Process Outsourcing
CCA	Controller of Certification Authorities
CERT	Computer Emergency Response Team
CIB	Central Informatics Bureau
CISD	Central Informatics Systems Division
COMESA	Commonwealth of Middle, East and Southern African States
COTS	Commercial Off the Shelf
CSO	Central Statistics Office
DBM	Development Bank of Mauritius
DOI	Digital Opportunity Index
DPC	Data Protection Commissioner
EGC	eGovernance Cell
EID	Electronic Identification Systems
EM	Enterprise Mauritius
ETA	Electronic Transactions Act
EU	European Union
GoM	Government of Mauritius
GPS	Global Positioning System
HORTIS	Horizontal Transfer of Indigenous Solutions
HRDC	Human Resource Development Council
IBA	Independent Broadcasting Authority
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Authority
ICTAC	Information and Communication Technology Advisory Council
IMC	Inter-Ministerial Committee for the Implementation and Monitoring of the NICTSP
IS	Information Security
ISP	Internet Service Provider
ITES	Information Technology Enabled Service
ITS	Information Technology Service
ITSU	Information Technology Security Unit
MACOSS	Mauritius Council of Social Services
MAGRIS	Mauritius Agricultural Resource Information System
MDG	Millennium Development Goals
MISCC	Ministry of Industries, SMEs, Commerce and Cooperatives
MITIA	Mauritius IT Industry Association
MITT	Ministry of Information Technology and Telecommunications
MoAC	Ministry of Arts and Culture
MoAF	Ministry of Agro-Industry and Fisheries
MoEHR	Ministry of Education and Human Resources
MoHQL	Ministry of Health and Quality of Life
MoLIRE	Ministry of Labour, Industrial Relations and Employment
MOST	Mauritius Offshore Services Team
MoTL	Ministry of Tourism and Leisure
MoWRCDPC	Ministry of Women's Rights, Child Development and Consumer Protection
MPL	Mauritius Posts Ltd
MQA	Mauritius Qualifications Authority
MT	Mauritius Telecom
MTPA	Mauritius Tourism Promotion Authority
NCB	National Computer Board

NGN	Next Generation Network
NGO	Non-Governmental Organisation
NICTAM	National Information and Communication Technology Authority of Mauritius
NICTERN	National Information and Communication Technology Evaluation and Research Network
NICTSP	National Information and Communication Technology Strategic Plan, 2007-2011
NRI	Network Readiness Index
NWEC	National Women Entrepreneur Council
OEM	Original Equipment Manufacturer
PCT	Programme Committee/ Taskforce
PIAP	Public Internet Access Point
PKI	Public Key Infrastructure
PoC	Proof of Concept (Prototype)
PPP	Public Private Partnership
RFID	Radio Frequency identification Device
RFP	Request for Proposal
SADC	South African Development Community
SBU	Strategic Business Unit
SEHDA	Small Enterprise and Handicrafts Development Authority
SIMC	Secretariat to the Inter Ministerial Committee for the NICTSP
SLA	Service Level Agreement
SLO	State Law Office Mauritius
SME	Small and Medium Enterprise
SMEF	Small and Medium Enterprises Federation
SMME	Small Medium and Micro Enterprise
TEC	Tertiary Education Commission
UNCITRAL	United Nations Convention on International Trade and Law
UNDP	United Nations Development Programme
UoM	University of Mauritius
UTM	University of Technology Mauritius
WWTE	Worldwide Travel Exchange

About the Exercise

The NICTSP was an extended collaborative exercise carried out from October 2006 to July 2007 involving ten Working Groups in the areas of ICT Domestic, ICT Exports, ICT Manpower Development and Planning, eGovernance, ICT for Social Development, ICT for Sectoral Exploitation, Information Security, Emerging Technologies Applications and Standards, Infrastructure and Electronic Communications, ICT Policy Regulatory and Institutional Framework.

PricewaterhouseCoopers India was the global consultant appointed for the exercise.

The exercise was supervised by the Technical Advisory Committee, chaired by the Chairman, National Computer Board, Mauritius and reviewed by a Steering Committee, chaired by the Hon'ble Minister, Ministry of Information Technology and Telecommunications, Government of the Republic of Mauritius, and co-chaired by the Country Head, United Nations Development Programme, Mauritius.

The exercise resulted in three main deliverables besides several working papers in the interim. The three main deliverables were

- The Final Analysis Report;
- The Strategic Framework Report; and
- The Action Plan Report.

NICTSP

2007-2011

