TRPC

C/M/S/
Law.Tax

LINCOLN LEGAL SERVICES (MYANMAR) LIMITED

Myanmar Cyber Legal and Policy Framework

Policies Related to e-Government, e-Commerce, and Cyber Security

(Draft - 25 Jan 2019)

Table of Contents

Executive Summary of Myanmar Cyber Law, and Policies Related to e-Government, e-Commerce, and Cyber Security

Introduction to the Project

The objective of the project is the development of an enabling policy, legal and regulatory framework for the Myanmar's ICT sector reform agenda. The **Cyber Legal and Policy Framework ("Framework")** will promote trust in the System, Infrastructure and Services provided by Government and Private Sector while addressing the following cyber-related objectives:

(a) to promote e-Commerce and cashless digital ecosystem,

(b) protecting Personal Data from misuse and align with international standards,

(c) protecting critical national infrastructure and related industries from cyber-attacks,

(d) discouraging and punishing cyber criminals from hacking systems including non-critical infrastructure.

Structure of the Cyber Legal and Policy Framework

The Cyber Legal and Policy Framework has been developed following (1) a first stakeholder consultation with stakeholders on 7 December 2018 in Nay Pyi Taw, (2) interviews with relevant and related officials and ministries during Project Trip 1 between 4-12 December 2018, as well as (3) an international benchmarking exercise against global best practices and indices for cyber legal and policy frameworks.

The Framework is presented in two parts - (1) **Myanmar Cyber Law**, and (2) **Policies Related to e-Government, e-Commerce, and Cyber Security.** These documents frame the project's three core categories of cyber policy, with its 15 related factors[1]:

1. e-Government - The Myanmar Cyber Law sets out legislation for e-Government in Part (III), including roles and functions of the existing e-Government Steering Committee, the e-Government Implementation Working Group, the e-ID Working Committee. Accompanying it is a proposed **National ICT Strategic Plan**, complementing the work of the "Myanmar e-Governance Master Plan 2016-2020"[2], to be implemented under the guidance of the existing e-Government Steering Committee. The National ICT Strategic Plan will address the core issues under e-government, including (A1) electronic information and online services, (A2) standardization, (A4) human resource development, and (A5) open government data

[1] Cyber Legal and Policy Framework Issues, as defined in this project: (A) e-Government: A1 Electronic information and online services, A2 Standardization, A3 Building information infrastructure, A4 Human resource development, A5 Open government data and open source software, A6 Intellectual Property Rights; (B) e-Commerce: B1 Cross border transfer of information by electronic means, B2 Electronic settlement, B3 Paperless trading, B4 Custom duties, B5 Online trade; (C) Cyber Security: C1 Privacy and data protection, C2 Exposure to cyber threat and cybercrime, C3 Electronic authentication, C4 Electronic signatures.

[2] https://www.motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%20%282016-2020%29%20English%20Version%28Draft%29.pdf

and open source software. Amongst other strategies, the National ICT Strategic Plan includes three sub-policies which may be considered separate policy documents: the **Government Cloud First Policy**, the **Data Classification Framework**, and the **Open Data Policy**.

One of the core issues under e-government has been defined as (A6) intellectual property rights, which is currently undergoing a **legal review and update exercise.** In February 2018, the Upper House of the Parliament of Myanmar, adopted the Trademark Bill, Industrial Design Bill, Patent Bill and Copyright Bill. The Copyright Bill was passed to the Lower House, which proposed amendments and returned it to the Upper House in September 2018. This update exercise is ongoing, and instead of developing further legislation which may clash and duplicate recent efforts, we recommend that this process continue as planned, if not accelerated.

Another core issue which has ongoing work under consideration is (A3) building information infrastructure, which is currently being developed through **Universal Service Fund (USF)**[3] under the umbrella of the Post and Telecommunications Department (PTD) of MoTC. The USF Management Board has been proposed in December 2018 and is awaiting cabinet approval (this remains unconfirmed at time of printing). The USF is used to roll out telecommunications and internet connectivity to all areas of Myanmar, and instead of creating a new policy, we recommend that the PTD should continue and accelerate its work on using the USF for building Myanmar's information infrastructure.

Other issues involving building information infrastructure have also been captured in the **Telecommunications Masterplan 2015**[4], which has yet to be formally adopted. Instead of duplicating efforts and rewriting this Masterplan, we recommend that the Masterplan be adopted, including the recommendation to set up the PTD as an independent telecommunications regulator, which in line with global best practices.

2. e-Commerce - The Myanmar Cyber Law sets out legislation for e-Commerce under Part IV, including references to include and/or adopt international standards, and suggestions of updates to other existing laws *such as the Electronic Transactions Law the Evidence Act)* to align them with the *UNCITRAL Model Law on Electronic Commerce*, and the *UNCITRAL Model Law on Electronic Signatures.* In addition,

[3] https://www.motc.gov.mm/sites/default/files/Universal%20Service%20Strategy%20%28Draft%29_0.pdf
[4] http://www.mcit.gov.mm/content/draft-telecommunications-masterplan.html

given the cross-cutting issues involved in developing and enhancing the e-Commerce industry in Myanmar, we recommend that an **e-Commerce Steering Committee** be established to address the core issues for e-Commerce, which include (B1) cross border transfer of information by electronic means, (B2) electronic settlement, (B3) paperless trading, (B4) custom duties, (B5) online trade, and also (from issues listed originally under the cyber security component): (C3) electronic authentication and (C4) electronic signatures.

3. Cyber Security - The Myanmar Cyber Law addresses cyber security in Part (V), proposing the **National Strategy for Cyber Security**, including Regulations for the Protection of Critical Information Infrastructure. In addition, the Myanmar Cyber Law sets up a **Personal Data Protection Commission (PDPC)** in Part VI, addressing issue (C1) privacy and data protection. The Myanmar Cyber Law also provides legislative foundation for **Computer Misuse and Cybercrime** in Part VII, addressing issue (C2) exposure to cyber threat and cybercrime. A Cybercrime Working Committee has also been proposed.

Next Steps

Both parts of the Myanmar Cyber Legal and Policy Framework - (1) Myanmar Cyber Law, and (2) Policies Related to e-Government, e-Commerce, and Cyber Security - will be distributed for further stakeholder and public consultation during Project Trip 2, scheduled to be on the week of 18 Feb 2019. There will be two stakeholder consultations:

- Stakeholder Consultation on 19 Feb 2019 Tuesday in Nay Pyi Taw, with the stakeholders expected to be primarily from the government and ministries,
- Public Consultation on 21 Feb 2019 Thursday in Yangon, with the stakeholders expected to be primarily from the private sector and non-government sector.

Myanmar Cyber Law (Draft)

Please see separate document.

Part I: Policies Related to e-Government: National ICT Strategic Plan

Introduction:

Myanmar's visionary leadership has understood that an advanced ICT sector is crucial to a growing, innovation-based economy. ICT will support all aspects of Myanmar's sustainable economic development.

This National ICT Strategic Plan builds on the progress Myanmar has been making over the past several years. It reaffirms the government's commitment to accelerating efforts at creating a vibrant ICT sector that supports and empowers people. Several programmes and policies outlined in this ICT plan are vital to Myanmar's future development. It will invest in improving connectivity through advanced ICT infrastructure.

The delivery of government services through ICT is key for Myanmar's progress. This Plan ensures the development of public sector ICT capacity and the use of innovative applications and programmes to improve public services. Recognising the benefits of cloud computing services, Myanmar Government will be adopting a cloud-first policy, along with a data classification framework for information security management. In line with open government data efforts that increase interoperability and openness, the Government is launching an Open Data policy. These efforts will drive innovation and productivity in Myanmar, improve security of information and enable growth in the digital economy.

To meet these goals, a comprehensive, strategic framework has been developed. It is organised into five strategic thrusts – the critical components needed to create a sustainable digital future. These thrusts will enable Myanmar to become a leading knowledge-based economy, and they are aligned with the government's broader national goals.

1. **Enhancing Public Service Delivery** – Information and Online Services, Standardisation
2. **Improving Connectivity** – Information Infrastructure
3. **Boosting Capacity** – ICT Human Capital and Intellectual Property Rights
4. **Advancing Government ICT** – Cloud First Policy, Data Classification Framework
5. **Fostering Openness** – Open Data Policy

The following section outlines the ICT Strategic Plan in greater detail, highlighting the initiatives and policies that each strategic thrust proposes.

1. Enhancing Public Service Delivery (A1, A2)

Information and Online Services (A1)

1. The online delivery of information and services by public agencies to the citizens, is a key feature of e-Government. There are an increasing number of information and transaction services available online, with additional ones being developed.
2. The E-Government Steering Committee is responsible for "encouraging enhanced productivity, efficiency and effectiveness in public services via the use of technology, online services and electronic information" (see Myanmar Cyber Law.)
3. The E-Government Steering Committee will guide the government in using innovative ICT applications to improve efficiency and provide new transactional and information services, increase coordination between government agencies and ministries and creating greater awareness of these services.
4. The E-Government Steering Committee will continue to work on increasing the number of resources available on the Myanmar National Portal and other online resources[5] (identified in the Benchmark Study Against Global Indexes), to increase government connectivity and transparency.

Standardisation (A2)

1. Standards lay the foundation for efficient government operations and services. With multiple agencies introducing e-government initiatives in Myanmar, standards will help ensure consistent, seamless and secure exchange of information between the government and end users.
2. In this regard, three initiatives will be taken:
    a. Establish an official standardisation body, which aligns its efforts with that of the E-Government Steering Committee, as per the powers awarded to the Committee by the Draft Myanmar Cyber Law to develop and issue guidelines on cybersecurity standards [Chapter (III) Section C/12/a]. This body will establish, monitor and coordinate standards development in the country and participate with international standard setting bodies.
    b. Implement internationally recognised standards within government agencies and CIIs (see National Cybersecurity Strategy).[6]

[5] Myanmar Law Information System, Myanmar National Trade Portal, Myanmar Industry Portal, government agencies and websites.

[6] These standards may include: International Organisation for Standardisation (ISO), International Telecommunication Union (ITU), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), Alliance for Telecommunications Industry Standards (ATIS), Organisations for the Advancement of Structured Information Standards (OASIS), 3rd Generation Partnership Project (3GPP), Interactive Advertising Bureau (IAB), Internet Society (ISOC), Industry

    c. Initiate a “Baseline Plus” Approach for cybersecurity standards (see Section 6, Baseline Certifications, Initial Standards and Protocols, Myanmar Cloud First Policy)

2. Improving Connectivity (A3)

Information Infrastructure (A3)

1. The Myanmar Government aims to deploy an advanced, secure infrastructure. Building on its progress in the last few years, it will provide increased access to high-speed, high-capacity infrastructure that is safe and secure.
2. This is currently being developed through **Universal Service Fund (USF)**[7] under the umbrella of the Post and Telecommunications Department (PTD) of MoTC. The USF Management Board has been proposed and is awaiting cabinet approval in December 2018 (this remains unconfirmed at time of printing). The USF should be used to roll out telecommunications and internet connectivity to all areas of Myanmar, and the PTD should continue and accelerate its work on using the USF for building Myanmar’s information infrastructure.
3. The Telecommunications Masterplan 2015 captures other issues involving information infrastructure. After formal adoption, it should be fully implemented and PTD be made an independent telecommunications regulator, in line with global best practices.

3. Boosting Capacity (A4, A6)

ICT Human Capital (A4)

1. The Myanmar Government aims to enhance digital literacy and develop the necessary skills in its workforce to enable innovation and participation in a knowledge-based economy. This will require a coordinated national effort focusing on education and training programmes.
2. More specifically, these efforts will include:
    a. Initiating a targeted human capital development programme aimed at strengthening the ICT skills among government employees.
    b. Guiding private and public educational institutions to develop ICT curriculum.
    c. Mandating companies to provide on-the-job ICT training to employees.
    d. Encouraging recruitment in the ICT sector and raising its profile as an attractive career path.

Specification Groups (ISG), Indian Standards Institute (ISI), European Telecommunications Standards Institute (ETSI), Information Security Forum (ISF), Request for Comments (RFC), International Standards for Auditing (ISA), International Electrotechnical Commission (IEC), North American Electric Reliability Corporation (NERC), National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS), and Payment Card Industry Data Security Standard (PCI DSS).

[7] https://www.motc.gov.mm/sites/default/files/Universal%20Service%20Strategy%20%28Draft%29_0.pdf

Intellectual Property Rights (A6)

1. The creation of a thriving digital economy will be dependent on fostering an entrepreneurial environment where content and creations are protected. Therefore, it aims to create an intellectual property regime that is balance and supports value-creation.
2. The intellectual property rights are currently undergoing a legal review and update exercise. In February 2018, the Upper House of the Parliament of Myanmar adopted the Trademark Bill, Industrial Design Bill, Patent Bill and Copyright Bill. The Copyright Bill was passed to the Lower House, which proposed amendments and returned it to the Upper House in September 2018. This update exercise is ongoing and should continue as planned.

4. Advancing Government ICT (A1-A6)

With the aim of advancing government ICT, the Myanmar Government has developed policies to improve data-sharing among agencies, save costs, allow government to focus on e-government efforts, and improve the security of data resources. These include:

i) Cloud First Policy

ii) Data Classification Framework

Myanmar Cloud First Policy

Section 1: Why have a Cloud First Policy?

The Myanmar Cloud First Policy complements the Myanmar e-Governance Master Plan[8]. It is designed as a "cloud first" policy - i.e. encouraging governments to use cloud computing solutions as their first option of choice, rather than building independent systems in silos.

Taking a cloud first policy approach addresses the rapid changes in technology use in the Myanmar government, who are already using cloud computing for their ICT needs. Having a cloud first approach also enhances the interconnectivity and interoperability of modern government ICT systems.

The Government of Myanmar recognises the full benefits of cloud computing services in driving innovation and productivity, developing and delivering citizen services more effectively, and more responsively to business and community needs, increasing speed and agility, increasing security, while at the same time realising efficiencies and cost savings.

A Cloud First policy is the first step away from the government's legacy IT. A cloud first policy directs the government to consider cloud IT solutions before alternatives. Ultimately, government use of IT will reach the optimal state in which government enterprises are innovating using the latest public cloud offerings and running optimised "born in the cloud" solutions.

By promoting and accelerating cloud uptake and usage, the Myanmar government is leading by example – and this, in turn, will enable growth in the digital economy. Wide adoption of cloud computing in the public and private sectors will lay the groundwork for other technologies to be developed, which will in turn, further improve shared e-government services, a more digitally-enabled civil service, a digitally-empowered citizenry and grow our digital economy.

Cloud computing has brought forth a new and more efficient means of managing government IT resources. As such, all government levels, bodies and institutions are encouraged to actively adopt a "cloud first" approach. This document sets out general guiding principles for government ministries, agencies and departments to consider in adopting cloud computing solutions as a primary part of their IT planning and procurement.

[8] https://www.motc.gov.mm/sites/default/files/Myanmar%20e-Governance%20Master%20Plan%20%282016-2020%29%20English%20Version%28Draft%29.pdf

Ultimately, the government will become cloud native, the optimal end state in which government enterprises are innovating using the latest public cloud offerings and running optimised ‘born in the cloud’ solutions.

Agency Implementation

All government ministries, agencies, departments, including government owned corporations and educational institutions are encouraged to adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government services, except when it can be shown that an alternative ICT deployment strategy:

- meets special requirements of a government agency, and
- is more cost effective from a Total Cost of Ownership (TCO) perspective, and
- demonstrates at least the same level of security assurance than a cloud computing deployment.

Cloud Computing Benefits

Cloud computing is a holistic term encompassing ICT infrastructure, processing, storage, networks, operating systems and applications that are available on demand in variable quantities. A cloud-based model enables stronger budget control and greater agility in financing requirements.

Initially, the interest in Open Source Software was motivated by the government’s desire for flexibility as well as cost savings. This has been superseded by the utility model of cloud computing. The agility enabled by the cloud computing model allows governments to profit from highly variable demand. It is this that is fundamental to the cloud business model and it is what is fuelling the rapid expansion of new citizen services and enabling a new wave of public service innovation.

1. **Budget control with a utility-based “pay for what you use” model** – government agencies only pay for the resources consumed without having to over-provision based on future forecasts or seasonal peaks. The scalability of cloud computing services means systems usage can be scaled up or down throughout the year as required (e.g., around income tax due dates). The transparency of this utility-based pricing structure means that spending caps and alerts can also be implemented, providing budget control assistance.
2. **Decreased capital spending on ICT infrastructure –** outsourcing government services to cloud computing results in immediate reductions of large capital outlays for ICT infrastructure and maintenance costs. More common commodity solutions – including best of class services – are also made available to government agencies through cloud provisioning, and costs are managed on an operational basis. The

cloud first model enhances government ICT resiliency and security as version upgrades to both hardware and software are managed by the cloud service provider (CSP).

3. **Faster deployment of services** – reducing the amounts of on-premise ICT infrastructure required to be built and owned by government agencies reduces overall deployment times and shifts the focus from management of infrastructure to delivery of services. Public cloud ICT facilities and services can be tested and deployed quicker, and maintained more cost effectively, than if government agencies own and run unique computing facilities themselves.
4. **Inter-agency collaboration for greater efficiency and better citizen services** – cloud enables more effective collaboration as agencies more easily share resources and information across institutions, allowing for greater efficiency, entrepreneurship, and creativity in delivering public services.
5. **Operational continuity and business recovery –** with cloud data storage, management, and backups, data retrieval and business continuity and recovery during times of crisis (e.g., natural disasters or other disruptive events) become faster, easier and more cost effective.

Section 2: Definition of Terms

This section covers several key concepts associated with cloud computing.

What is Cloud Computing?

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, five deployment models, and certain assurances.

Essential Characteristics[9]

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

[9] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- **Resource pooling.** The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and re-assigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

Cloud Deployment Models

- **Private.** The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.
- **Virtual Private.** The cloud infrastructure is provisioned for exclusive use by a single organisation based enhanced global security and compliance standards. It provides a virtual private cloud environment off premise with strong isolation and may provide dedicated infrastructure for exclusive use by an organisation.
- **Community.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Commercial.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

- **Hybrid.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).
- **Government Cloud**. A public service cloud infrastructure provisioned by the government for use by government agencies. This may itself include a variety of cloud deployment models (public, private, community, hybrid), each of which may be outsourced or owned by the government. Government cloud providers should be pre-accredited to provide services to ministries, agencies, departments, including government owned corporations and educational institution. Government cloud providers should meet a specific minimum standard for providing services to government agencies. (See Accreditation Process.)

Assurance Approaches: Shared Responsibilities

In the context of the provisioning of cloud services, when a customer moves computer data or systems/applications to a cloud computing service, responsibilities are shared between the CSP and the customer. Within this context, the customer will be the contracting government agency, and the government agency will appoint a Government Data Manager to be responsible for the management of the data under the control of the agency (see, Data Classification System and Security Controls Framework).

Certain aspects of security, data protection and compliance continue to rest with the government agency, while other aspects are taken on by the CSP:

- The *cloud customer* performs a role like that of a data controller, as it controls its content and makes decisions about treatment of that content, including who is authorised to process that content on its behalf. Government agencies/ partners assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, configuration of security group firewalls, and other security, change management, and logging features.
- The *cloud service provider* performs a role like that of a data processor, as the service provider only uses customer content to provide the services selected by each customer to that customer and does not use customer content for other purposes. The CSP typically does not have control of or access to the cloud customer’s data. The CSP operates, manages, and controls the infrastructure components, from the

host operating system and virtualisation layer down to the physical security of the facilities in which the services operate

When evaluating the security of a cloud solution, it is important for government agencies to understand and distinguish between:

- Security measures that the CSP implements and operates: security of the cloud; and
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of cloud services: security in the cloud.

Typically, the CSP customer is implementing the logical security controls and the CSP is responsible for the physical security controls of the data centre. However, the level and nature of responsibility on both parties depends on the cloud deployment model type, and government agencies (i.e., customers) should be clear as to their responsibilities in each model.

Section 3: Security and Standardization

The benefit of migrating government workloads and data onto commercial cloud is the ability to enhance overall data security. Cloud service providers will meet international security standards (such as the Payment Card Industry (PCI) Data Security Standard (DSS)), will be certified appropriately (such as ISO9001, ISO27001), and will abide by all relevant industry standards.

We recommend that government agencies develop a protective security policy – a Security Controls Framework – which applies a risk management approach towards its own data control requirements (see, Data Classification Framework). and align this with international standards and certifications, as well as industry standards. The precise level of security requirements for contracted cloud services should be determined by the contracting agency based on an assessment of data risk. Stipulated security controls can include any one or more of the following:

- Physical and environmental security
- Business continuity management and incident response
- Inventory and configuration management
- Data encryption
- Access controls, monitoring and logging
- Network security and monitoring.

To implement a security controls framework that is appropriate for a Cloud First environment, government agencies need to first understand that security in the cloud is a shared responsibility between the contracting government agency and the CSP.

Data Sovereignty

The benefits of cloud are best realised when there are no data residency restrictions placed on data. Such restrictions undermine the economies of scale and security benefits to be gained from shared computing infrastructure. Access to data in the cloud is dependent on security controls, and agencies concerned with extraterritorial access to data owned by the government should select cloud vendors with the appropriate security standards and controls.

Security Framework

Managing the security of contracted cloud services is a responsibility that is shared between the contracting agency and the cloud service provider, with the contracting agency defining security controls in the cloud, while the cloud service provider is responsible for the security of the cloud.

Data security depends upon: (1) Meeting security requirements for each data classification level; and (2) Employing standardized tools and procedures for audit*.*

Data that can be migrated to the commercial cloud will need to meet security requirements for accreditation and be verified by international cloud security standards. Accepted international security standards include ISO 27001, Service Organisation Controls Report (SOC) 1 and 2, Payment Card Industry Data Security Standard (PCI DSS), and Cloud Security Alliance (CSA) certification and audit, or their successors. Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits or higher), ECC (160 bits or higher), and ElGamal (1024 bits or higher) or their successors.

Commercial cloud service providers should provide logical security audit on data access, including logs and audit trails to ensure the prescribed security and privacy requirements are met.

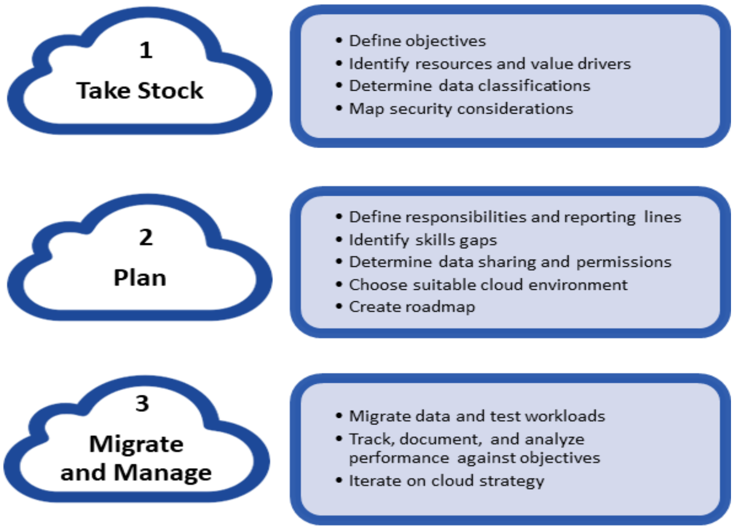
Government agencies should rely on logical audits and continuous security monitoring to ensure cloud services meet the agreed-upon data confidentiality and integrity, that there have been no data breaches, and that data and workloads are continuously available.

Agencies should refer to the Data Classification Framework for further detail.

Section 4: Migration Policy

Migrating data and workloads to the cloud enhances the availability and functionality of services and improves interoperability. Migration to cloud also enables greater automation of certain processes, increasing the availability and agility of computing resources for processes that have variable processing demands.

Migration can be seen as a three-step process: (1) Take stock (2) Plan (3) Migrate and manage.


1
Take Stock
• Define objectives
• Identify resources and value drivers
• Determine data classifications
• Map security considerations
2
Plan
• Define responsibilities and reporting lines
• Identify skills gaps
• Determine data sharing and permissions
• Choose suitable cloud environment
• Create roadmap
3
Migrate and Manage
• Migrate data and test workloads
• Track, document, and analyze performance against objectives
• Iterate on cloud strategy

1) Take stock

Identify how IT resources are aligned to objectives, and how costs are optimised. Take stock of entity data classifications and the corresponding security considerations, the degree to which the risks are regarding confidentiality, integrity or availability. Non-sensitive workloads and those that pose low security concerns should be prioritised for migration first. Government websites, public archives, development and testing environments, are more readily moved to the cloud.

The value of moving workloads to the cloud is determined by the technology lifecycle and the increased functionality that cloud can bring. Moving workloads from IT resources that are near the end of their current technology lifecycle can avoid costly investments in new IT resources.

2) Plan

Create a roadmap for migrating service to the cloud, including defining responsibilities and reporting lines. Migrating workloads to the cloud can change the skills needed within the organisation, for example by requiring more developers and engineers, and fewer people concerned with managing IT infrastructure. This means working with cloud providers to understand the staff skills, training and education needed in the migration and post-migration workloads.

- Identify data that can be shared, and would benefit from being shared, and requirements on security and access permissions for such data.
- Identify the suitable cloud environment, such as virtualisation of legacy IT, performance and functionality requirements, costs, and compatibility with legacy IT.
- Determine whether replacing existing applications with new ones or to redesign service delivery architecture from the bottom-up is preferred.

Contracted cloud services should be able to integrate with existing services and should be interoperable with locally provisioned IT. They should be contracted on an aggregated basis to meet planned data and workload migration needs.

3) Migrate and Manage

Track, document and analyze progress of the plan in an incremental and iterative manner. Monitor performance and service delivery against objectives and compare costs against the migration plan.

Following migration, adequate testing of the cloud environment needs to be performed before existing solutions are decommissioned. Testing should be performed on the basis of both typical/normal usage scenarios and extraordinary utilisation/demand scenarios.

Ensure that staff are trained in the contracting and management of cloud services through service level agreements (SLAs) with cloud vendors and possess the requisite skills to manage the migrated workloads.

Section 5: Data Ownership, Retrieval, and Interoperability

Data Ownership

Government institutions retain full control and ownership over their data. This is ensured through the Cloud Service Provider identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity.

Service contracts and other service level agreements (SLAs) related to provisioning of cloud services for Government agencies shall clearly provide that any data migrated to the cloud remains the property of the contracting Government entity, regardless of who owns, manages or operates the cloud. The contracting agency will retain rights of data access, retrieval, modification and deletion regardless of the physical location of the cloud services, including the right to approve, deny and revoke access by third parties, and the right to determine the geographic location of the data.

Access

Access, retrieval, modification and deletion of data remains the right of the contracting Government agency and will be reflected in the relevant service contracts. The policies and processes pertaining to data access will be defined according to the needs of the contracting entity and specified in the agreement between the Government agency and the cloud provider.

Interoperability

A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in, and CSPs should allow customers to move data on and off of their cloud platforms as needed. Interoperability of the components of an on-premise infrastructure should be put in place based on international standards, such as ISO/IEC 17203:2011 Open Virtualisation Format (OVF) specification.

A cloud system's components may come from different sources including public and private cloud implementations. These components should be replaceable by new or different components from different providers and continue to work, to facilitate the exchange of data between systems. CSPs are required to provide interoperability, ensuring government agencies may be able to change CSPs easily without a lengthy procurement and implementation cycle.

Section 6: Accreditation Process for CSPs

Accreditation

An accreditation process for CSPs will be laid out by the Information Technology and Cyber Security Department (ITCSD). The accreditation shall provide for baseline requirements necessary for most government IT procurements, and thereby inclusion on the Accredited CSP List. This is to ensure basic levels of service reliability from CSPs, and to assure that they have secure and controlled platforms providing the necessary array of security features which government agencies can use. International best practices have shown accreditation can be done one of two ways: (1) by local accreditation with local standards, or (2) by obtaining international certifications. Agencies should ensure that they only consider vendors who are on the Accredited CSP List.

“Baseline Plus” Framework for Certifications, Initial Standards and Protocols

Agencies should also look towards selecting a CSP with baseline certifications, standards, or protocols which match their functional requirements. Some examples of matching an agency’s required function, and the baseline certification or protocol required include the following:

CODES OF PRACTICE	BASELINE CERTIFICATION AND/OR PROTOCOL REQUIRED
Controls	Protocols: OAuth, Security Assertion Markup Language (SAML) Optional: Service Organisation Control (SOC) 1 and 2
Information Security Management	Certification: ISO/IEC 27001 - Information Security Management
Personal Data	Compliance with the [Myanmar Law Protecting the Privacy and Security of Citizens] Optional: ISO 27018 Certification
Electronic Payments	Payment Card Industry (PCI) Data Security Standard (DSS)

Further information on baseline certifications and required protocols will be provided by ITCSD.

Technical and Sector-Specific Certifications

The Accreditation system may expand beyond baseline accreditation, to be based on the anticipated heightened requirements of certain agencies, sectors or for certain types of data, and therefore, include tiers of accreditation aligned with the specific class of requirements.

For example, individual sectors will have specific certifications required. It is important that all certifications are based on existing international industry standards and certifications. These should be considered in tandem with the baseline certifications required, depending on the government agency’s requirements. Notable examples are regarding national defence or national security information, or health information.[10]

[10] In the US, all health information held by the government or the private sector are subject to the data protection requirements of two US national laws, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH). There are industry certifications for cloud services that accredit CSPs as HIPAA and HITECH compliant.

Section 7: Public Procurement Process

Making the procurement of cloud computing services as simple, consistent across government and robust as possible for government agencies is crucial to the success of the cloud first policy. Cloud services should be listed in such a way as to clearly show how a utility model for procurement and payment will function, thereby providing clarity in showing value for money in procurement.

A marketplace – or a common online platform that can be used by all government agencies – simplifies the cloud procurement process. A centralised e-procurement model ensures:

1. Vendors adhere to common accreditation requirements;
2. Increased transparency on cost and accreditation, which helps government agencies choose between similar services; and
3. Costs savings by avoiding the need to conduct a full market evaluation.

In consultation with government agencies, the government will develop a one-stop-shop marketplace, containing a wide range of pre-vetted vendors and services (in line with the Accredited CSP List). This marketplace approach will take into consideration security expectations and procurement challenges and will evolve to incorporate sector-specific accreditations.

Structuring Cloud Purchases for the Public Sector

Direct or indirect purchases of cloud can be undertaken by agencies:

- direct purchase from CSPs designed for commercially-available service, purchased as a commercial service item offered without labour hours;
- indirect purchase from a CSP partner or reseller, negotiating an agreement with that organisation.

There are four ways of purchasing cloud services:

1) Purchase from list of accredited cloud vendors and services

This enables a direct or indirect purchase of cloud services. A list of accredited cloud vendors and services which have met a minimum requirement should be kept by the ITCSD. This is similar to best practice approaches elsewhere used to ease and accelerate cloud adoption in the public sector, for example:

- Australia’s list of accredited cloud services vendors for their Whole of Government (WoG) Procurement Contracts, Arrangements and Initiatives – Cloud Services Panel[11]
- Singapore requires any CSP serving the public sector to be certified under the Singapore MTCS security standard[12]
- United Kingdom’s government cloud marketplace requires all digital suppliers to apply for eligibility and qualify under their Digital Marketplace Framework[13], before being able to be listed as a possible public service provider.

2) Leverage an existing vendor contract (indirect purchase)
Government agencies “share” a contract which has already been negotiated by another agency. Agencies can tap upon these pre-existing agreements if applicable.

3) Purchase from a CSP reseller (indirect purchase)
Government agencies buy directly from a CSP reseller or partner – they do not deal with the CSP directly. This could be due to the desire to purchase a bundled service or maintenance provided by the CSP reseller.

4) Issuing a Terms of Reference (TOR) or Request for Proposal (RFP) (indirect purchase)
A traditional procurement approach for end-to-end or turnkey solutions, Agencies put together a list of their requirements via a Terms of Reference or Tender and have CSPs as well as systems integrators propose solutions for purchase.

Building Infrastructure vs Renting Access: Utility-Based Pricing Models

Cloud computing brings the benefit of funding IT services as operational expenditure (OpEx) rather than capital expenditure (CapEx). While capital expenditures depreciate over time, a cloud-based OpEx budget allows for far stronger and more flexible budget control, having removed sunk capital costs.

Four elements are key for agencies to note when selecting CSPs: (1) transparency in pricing, (2) variable prices for different services, (3) multiple pricing models which allow agencies to evaluate CSP pricing against their organisational needs, and (4) pay-per-use utility model.

[11] http://www.finance.gov.au/policy-guides-procurement/cloud-services-panel/
[12] Singapore Infocomm Development Authority (IDA), 13 Nov 2013, New Multi-Tier Cloud Security (MTCS) Standard Launched in Singaporehttps://www.ida.gov.sg/About-Us/Newsroom/Media-Releases/2013/New-Multi-Tier-Cloud-Security-MTCS-Standard-Launched-In-Singapore
[13] United Kingdom, n.d., Digital Marketplacehttps://www.digitalmarketplace.service.gov.uk

CSP pricing should be via a pay-as-you-go model, possibly with a baseline cost for services, and additional resources used listed as separate items. CSPs should provide transparent, publicly-available, up-to-date pricing, and tools that allow customers to evaluate their pricing. They should also provide customers with the tools to generate detailed billing reports (with line-item breakdowns) to meet compliance needs. An example of a single-line item structure approach towards utility-based pricing is as follows:

ITEM NO	**SUPPLIES/SERVICES**	**QTY**	**UNIT**	**UNIT PRICE**	**AMT**
1001	CSP Cloud Services	1,000	EACH	USD1.00	USD1,000

Data Classification Framework

Introduction

The Myanmar Government is on a journey to implement ICTs to modernise operations, increase effectiveness, and deliver innovative services to citizens. Within this context, there is broad recognition that the unique properties of cloud-based services such as scalability, elasticity, cost management (paying only for what is used when used), and high levels of security often provide the best options. Similarly, for many of the challenges being faced by the government, such as exponentially increasing amounts of data that require processing and storage, escalating cyber threats, the push to reduce costs and improve efficiencies, and the government's desire to meet citizen needs in new ways, cloud services provide government with flexible solutions.

With new ICT technologies such as cloud computing, mobile devices, data analytics and artificial intelligence, come new opportunities and security challenges. Government has never before had the ability to make services accessible to so many citizens on an immediate, as-needed-when-needed basis. But with these opportunities come the need to make information security more resilient, refined and efficient. To meet these objectives, governments need to carefully consider how to take advantage of the benefits of modern computing systems and methods while keeping important data safe.

The Myanmar government has initiated its journey to the cloud with a ***Cloud-First Policy*** that clearly sets out goals and creates the conditions for achieving those goals. The policy includes a directive that the government develop a protective security policy – a Security Control Framework. The Security Control Framework takes account of both physical and logical information security. An important component of any comprehensive security policy is a policy for ***classifying data***, allowing Government Data Managers to appropriately protect different types of data, while discouraging wasting resources on unnecessary and costly security controls for less sensitive information.

With data classification and an understanding of the **security controls** necessary to protect data, the government can then identify or design and implement **appropriate controls** relative to the level of security needs for a particular classification, and to ensure that they are **operating effectively** on an ongoing basis. A robust **risk assessment** framework well implemented will align risk to sensitive data with security controls and maintain the validity of security controls.

Overview of the Data Classification Framework Policy

Not all data is equal. Information security management could become overwhelming and unaffordable for an organisation were one to secure all information in the same manner. Some information is sensitive or likely to be sought for illegal or dangerous purposes. Other information has no risk associated with its wide dissemination. *Data classification is a means to characterise information according to the risks associated with unauthorised dissemination of that information and the risk of threat certain information may attract.* By distinguishing information based on risk, an enterprise can implement the security measures commensurate with the risk. The reality is that most government organisations handle very little highly sensitive information. For example, the UK government estimates that 90% of government information falls within the lowest security classification for their data.

Typically, the fewer the levels of classification, and the clearer the distinctions between levels, the more effective the classification system will be in properly securing the most sensitive information. For government, this serves the public interest in two key ways: First, truly sensitive information is appropriately secured; second, the largest portion of government information is available to the public consistent with transparency and open government, as well, it is available for productive secondary uses for those other than government to provide services or contribute to the public good.

Of course, when an organisation is responsible for classifying its information, there is a risk of over-classification, securing information that in actuality need not be protected from disclosure. Over-classification can result in an overall weakening of security defences by spreading the focus of, and budget for data security over a much broader set of systems and data than is actually necessary. On the other hand, under-classification inadequately protects information and systems commensurate with the risks associated with disclosure or the threats that may lead to the malicious modification or destruction of the information. So, it is critical when implementing a data classification system, that the categories be clear and those responsible for classification understand the distinctions between classifications and most importantly the goals for classification.

There are two connected requirements in this policy approach:

- **Data Classification:** identifying the risk associated with particular government data.
- **Security Framework**: ensuring clear security control requirements that correspond to the level of risk associated with particular government data and applying those across government.

This policy is thus divided into two related perspectives, first considering data security from a data classification perspective, setting out a data classification system that will enable Government Data Managers to prepare their data for secure storage on IT systems. The second section provides for a Security Control Framework by which Government Data Managers can work with Cloud Service Providers (CSPs) to align security controls to the level of sensitivity of the government data.

For each government organisation, an individual, herein referred to as the “Government Data Manager” is responsible to lead the team within the organisation that is to lead the processes of data classification and implementation of security controls in accordance with this Policy. The Government Data Manager is responsible for the security of data created, maintained or otherwise managed by their respective government organisation.

Introduction to Data Classification

It is important for each organisation to identify an individual responsible for data management and controls for the organisation. The individual, herein referred to as the “Government Data Manager”, is responsible for leading the processes of data classification and implementing security controls in accordance with this Policy. The Government Data Manager is responsible for the security of data created, maintained or otherwise managed by the respective government organisation.

Governments have long needed to be able to distinguish highly sensitive information from that which is either less or not sensitive. A clear delineation of data requiring high levels of security better positions a government to benefit from ICT and cloud investments, delivering better services to citizens at a lower cost. Any Security Control Framework depends on the effective classification of new data. The person or team responsible for classifying new data performs a risk assessment for data that is being generated by the organisation. Depending on the institutional risk associated with the data, and the value, sensitivity and criticality of the data, the data can be classified into the appropriate category. Access controls and minimum-security requirements will need to be established for the handling and management of data within each data classification.

Most government organisations handle relatively little *highly* sensitive information. This fact underlies why many governments, including the government of Myanmar, are adopting a “cloud-first” policy for ICT procurement. But there must be appropriate security even for lower-risk but important information. **This policy guides the government to parse the**

information into classifications, ideally securing only that information that must be protected, and protecting the information at the appropriate level of security.

Fundamental Principles of a Data Classification System

The starting place for classification is **a *taxonomy*** by which an agency can categorise information. The taxonomy is usually implemented with sufficient guidance so that individuals properly align the security needs of the data with the requirements for each classification. Typically**, the fewer the levels of classification, and the clearer the distinctions between levels, the more effective the classification system** will be in ensuring the most sensitive information is properly secured.[14] This serves the public interest in two key ways: (i) truly sensitive information is appropriately secured and (ii) resources are not wasted on securing other information.

Over-classification can result in an overall weakening of security by spreading an organisation's data protection defences over a much broader set of systems and data than is necessary. On the other hand, under-classification can inadequately protect against loss of data or malicious modification of data. So it is important when implementing a data classification system, that the categories be clear, and the procedures and goals for classification are fully understood.

Consistency across government is important. The greater the consistency in classifying information across government, the more efficiently cloud services can be aligned with information security needs.[15] Clear, consistent classification across government also enables government-wide consistency. Pursuant to the Cloud First Policy, the Information Technology and Cyber Security Department (ITCSD) will establish a cross-government programme for CSP certification and an online marketplace for government agencies to procure appropriately certified cloud services.

As a government develops and applies a classification scheme, it is important to maintain focus on the goal: to **ensure that information is *appropriately* secured.** To achieve this goal, a classification process should identify the risk associated with particular information, distinguish information that requires a higher level of security from that which requires less or no specific security, and set an appropriate security level to properly protect the information.

[14] This is evidenced by recent changes in classification in the UK, with the government streamlining from six to three classifications and clarifying the characteristics for each.

[15] For example: The US has taken measures to create far greater consistency in data classification by mandating standards for both information and information systems be set and overseen by the National Institute of Standards and Technology (NIST), and that these standards be adopted government-wide and overseen by a single agency, the National Archives and Registry Administration (NARA). Cross government certifications are illustrated by the US FedRAMP cloud procurement certification programme. FedRAMP certifies that a cloud service provider meets certain security requirements. Thereafter, a federal agency can procure services that are appropriate to its specific needs and security requirements knowing that the service provider meets FedRAMP requirements, reducing redundancy and therefore the cost of procurement.

The outcome will be greater information security with higher efficiency and commensurate cost savings.

Key Responsibilities for a Government Data Manager

The goal of data classification under this policy is to enable a Government Data Manager to implement the government's Cloud-First Policy. When considering the adoption of cloud computing, a Government Data Manager has three areas of responsibility:

- Classifying data by identifying the risk associated with particular government data
- Implementing a security framework that provides for clear security control requirements that correspond to the level of risk associated with particular government data and applying those across the government organisation
- Ensuring both the government organisation procuring cloud services and the cloud service provider understand their responsibilities with regard to security and risk management.

Classification of Data

A three-tier approach for an information classification system can ensure the appropriate level of security for government information while enabling government to adopt commercially available, modern ICT technologies such as cloud computing. The Myanmar government has adopted the following three-tier security classification system:

- **TOP SECRET** – requiring the highest degree of protection. Compromise of this data would be expected to cause exceptionally grave or catastrophic damage to the national interest, organisations or individuals as described by the classifying authority.
- **SECRET** – used when compromise of the data would be expected to cause serious damage to the national interest, organisations or individuals as described by the classifying authority.
- **GENERAL** – used when compromise of the data could be expected to have only limited adverse effect on organisational operations, organisational assets, or result in only minor harm to individuals. This may include information that is not critical to business needs or operations.[16]

GENERAL is the classification that applies to the bulk of secured government information. When evaluating whether to apply the GENERAL classification, the first step of the analysis is to look at the risk to the institution. The second step requires considering the security priorities for the information.

[16] Some information must be restricted to a certain audience. To address this, the classification system could have "caveats" for example, "PROTECTED-SENSITIVE" restricting access to a "need to know" basis, and "PROTECTED-EYES-ONLY" to specify a specific audience (e.g., an individual, a government unit or an agent of a foreign government) for the information.

In evaluating for the GENERAL tier, risk to the institution is assessed by considering:

1. Compliance with all applicable laws and government policies;
2. The risk of malicious access to or dissemination of information to harm the agency, government or other national interest; and
3. The potential value of the information to a malicious actor
    a. financial or other direct value of the information to a malicious actor
    b. adverse societal implications (such as harm to businesses, preservation of legal rights, or preservation of political stability).

In addition to three tiers of classified information, most government information will be **unclassified**, without significant (or possibly any) concern for risk were the information be accessed or disseminated. For this information, there may still be security concerns, but these concerns can be addressed typically with the standard security measures undertaken for an appropriate public cloud information system. For some unclassified information, the individual responsible for the security of the information will want to take appropriate measures that align with the need to protect the information, including obtaining provisions in a service level agreement (SLA) describing security measures.

Security Control Framework

The control framework for any ICT environment depends on **physical** and **logical security controls**:

Physical security controls comprise three aspects:

1. Restricting physical access of the ICT infrastructure to only those persons with appropriate permissions;
2. Ensuring that the ICT infrastructure is safe from physical and environmental risks, such as flooding and will remain operational (or will resume operations within an accepted delay) in the case of, for example, loss of electricity;
3. Planning and provisioning sufficient resources to meet the demand for ICT resources at all times.

Logical security controls comprise protocols and tools to restrict *data* access, including:

1. Classifying data according to risk
2. Defining security clearances for different data classifications
3. Defining security standards and user authorisation levels
4. Managing data according to the data classification

5. Implementing validation and audit procedures to ensure compliance with security controls.

Many of these responsibilities can be done by implementing and operating software-defined identification and authentication of individuals accessing data.

Cloud-based security control framework

With a cloud-based ICT environment, data security is a shared responsibility. The Government Data Manager may outsource much of the responsibility for physical security controls to their CSP. CSPs typically operate large-scale facilities that serve multiple customers. The economies of scale allow CSPs to implement stricter physical access controls than what can be feasibly implemented for on-premise ICT. CSP's data centres may also be able to implement more robust protections against environmental threats and human error, as well as failover switches that automatically provision redundant resources if a network resource fails.

CSPs can provision rapid or on-demand scaling of the ICT resources that are available – where it would typically take days, weeks or months to scale up an in-house ICT system. As a result, the physical security controls in a cloud-based system are typically more robust than on-premise ICT environments.

The physical security of customer data can be validated by referring to international standards. To this end, a Government Data Manager should look to select CSPs that comply with international cloud and information security standards, such as, the Cloud Security Alliance's *Cloud Controls Matrix v3.0* (CSA CCM v3.0)[17] or the International Organisation for Standardization's ISO/IEC 27001[18] for information security management systems for reliable assurance that their cloud infrastructure is secure. CSP compliance with international standards can then be audited by an independent third party.

By referring to international standards and third-party compliance audits, a Government Data Manager can be confident that their contracted cloud services meet requirements for security and reliability. The Government Data Manager should also ensure that any cloud SLAs include service availability commitments.

[17] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/
[18] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

There may be some information for which the customer cannot rely on third-party, outsourced physical security controls – e.g. TOP SECRET data. In these instances, cloud services may not be the appropriate solution.

Defining security controls

In a cloud environment the control framework of the Government Data Manager will be responsible for logical controls, including:

- Data classification;
- Defining and monitoring access controls for the cloud platforms and applications;
- Implementing and operating appropriate data management and encryption;
- Preventing risks associated with software security;
- Managing personnel security;
- Monitoring cloud performance; and
- Continuity planning, incident handling and event logging.

Examples of widely used logical security controls are described below:

- Encryption: A fundamental security control is encryption. Encryption applies when data is either at rest, or in transit. Depending on the classification, it may be appropriate to encrypt data which is “at rest,” by encrypting individual files or the entire drive where the files are stored. It is also a best practice to encrypt data “in motion,” encrypting data which is in transit. Encrypted “in motion” means using encrypted channels for transferring data. For web-based transfers, this implies implementing encryption using a third-party certificate from a trusted vendor.[19]
- Password Access Control: The most common access control is to rely on passwords for data access and enhance security. However, mandating long and complex passwords and frequent changes to the passwords in use may increase the risk that authorised users handle their passwords badly, for example, by writing them down or storing them in an insecure location. This can reduce the ability of passwords as security controls to serve their intended purpose.
- Enhanced Access Control: Multi-factor authentication has emerged as a popular alternative to complex password routines, whereby access is granted upon authentication of two or more components that confirm the identity of the user. Common implementations include a combination of two or more factors such as a static PIN code, a code sent to the user via SMS, or a dynamic password generated by a mobile application or dedicated security device.

[19] This results in the “s” in “https” on web-addresses such ashttps://www.domain-name.com/

- Log-in Monitoring: Data managers can also actively monitor logins and authentications and implement automated, risk-based triggers to detect attempts at unauthorised access. Other security controls include limiting login sessions, automatically logging out inactive sessions after a predefined period of inactivity, and not authorising permanent logins.
- Access Audits: Auditing access to data can serve two purposes. Regular audits can aid in identifying a previously unidentified breach, and specific cases of a breach or unauthorised disclosure, as a forensic tool to identify the source of the breach or disclosure.

Determining the appropriate measures should also ensure that security controls do not negatively affect usability of the service. If security controls make a service too difficult or cumbersome to use, then it may not be the *appropriate* security controls.[20]

As discussed with regard to the Security Controls Framework, security controls fit into two categories: Physical and logical controls. Physical controls are the responsibility of the CSP and must be addressed in the service level agreement (SLA) between the government data manager and the CSP.

Aligning Security Controls with Data Classification

A detailed discussion of this topic is presented in Section 5 of this Policy. SECRET or TOP SECRET data requires more rigorous security standards, while data classified as GENERAL requires basic security controls. Security standards can refer to international standards such as ISO 27001 for information security management systems,[21] ISO 27017 on cloud-specific information security controls,[22] and ISO 27018 on protection of personally identifiable information on public clouds, or to data classification models employed elsewhere that are deemed appropriate. Referring to international standards in the definition of minimum security for each data classification may help the customer readily assess which cloud services meet the level of information security and control required.

Assigning security requirements based on data classifications can reduce the cost of data management, facilitate more efficient usage and sharing of information within the organisation and between different organisations, and will help ensure that data is appropriately secure.

Defining and monitoring access controls for cloud platforms and applications

[20] Amended from UK Cloud Service Security Principles (Beta), see:https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
[21]http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[22]http://www.iso27001security.com/html/27017.html

Data migrated to the cloud is typically private by default, so the only person that can access the data is the owner of the data, i.e. the Government Data Manager. The Government Data Manager can grant access permissions according to a data access policy – essentially a list of categories of access rights, such as to read, modify or delete data.

While physical security controls are outsourced to the CSP, the customer, i.e., **Government Data Manager, retains control of the definition and management of access controls**. The Government Data Manager can grant, manage and revoke data access permissions as necessary, and retains responsibility for keeping permissions up-to-date. The Government Data Manager can also control how data is being used and decide what operating systems and software are used to manage the data on the cloud.

The Government Data Manager is responsible for permissions and can actively manage data access lists such that data resources are available to those that need the data – for example, to perform their work duties or as a matter of right-to-access public information. They can also manage lists such that people that are not supposed to access certain data are not able to access the restricted data.

Implementing and operating appropriate data management such as encryption
The Government Data Manager can choose to implement security controls for data during transfer, storage and processing. Such controls can also be defined with different security requirements for the different data classifications. Depending on the classification, these controls can include encrypting data “at rest,” by encrypting individual files or the entire drive where the files are stored, and encrypting data “in motion,” encrypting and decrypting data which is in transit.

The government data manager can control *where* the data is being stored, including potentially choosing the jurisdiction where the data is located. Cloud customers that transfer personal information or other data that is subject to restrictions on cross border data transfers will need to ensure their data is stored and processed by a CSP that complies with the necessary certifications and requirements. For example, a cloud customer transferring data from the EU to Singapore should ensure their CSP complies with the EU regulations and, to the extent necessary, has obtained approval from the EU data protection authorities for transferring personal data from the EU to a non-EU jurisdiction.

The Government Data Manager may also choose to require the CSP to disclose where data is being stored, processed and managed so that the cloud user understands which jurisdiction their data is subject to and the rules by which the data can be accessed without their consent – e.g. by government authorities.[23]

The Government Data Manager can control *how* data is being transferred and stored. This includes deciding whether data needs to be encrypted from end-to-end or only encrypted while it is stored, whether data masking is necessary, which creates similar but inauthentic versions of the original data before it is transferred and processed, and whether data needs to be anonymised by stripping all personal identifiers from the data before being transferred or processed.

Data will typically be encrypted "in motion" by using encrypted channels for transferring data. For web-based transfers, this implies implementing encryption using a third-party certificate from a trusted vendor.[24] **Increasingly, there is *no* reason to not use a secure, encrypted channel for transferring data –** the impact on performance is negligible and the data is more secure. Citizens' data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.[25]

Preventing risks associated with software security

The Government Data Manager, as cloud customer, retains control and responsibility for operating systems and software that they install on the cloud. To reduce the risks associated with software, the cloud customer can implement routines for regular installation of updates and security patches for operating systems and software applications running on the cloud.

Operating systems and software on the cloud that are not up to date are vulnerable to data breaches by unauthorised third parties in the same way that operating systems and software on in-house ICT systems are. The cloud customer can manage all applications that they install on the cloud according to the same security routines that they use for local servers and workstations.

Managing personnel security

A trusted insider with authorised access to ICT systems present one of the most malicious threats to an organisation, both in government agencies and commercial enterprises. Trusted employees may be targeted by third-parties looking for unauthorised access to

[23] The UK "Cloud Security Principles" recommends this approach. See:https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
[24] This results in the "s" in "https" on web-addresses such ashttps://www.domain-name.com/
[25] Extracted from the UK *Cloud Service Security Principles* (Beta), see:https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

information, or they may be (or become) self-motivated to access and share restricted information, e.g. for personal financial gain.

To manage personnel security risks, the Government Data Manager can focus on the same personnel screening and monitoring practices as those used for staff with privileged access to on-premise assets. This may include a certain level of screening new employees, implementing employee reviews to assess employees' continued employment, and conducting security and incident reporting training as appropriate. Personnel security management helps protect employees as well as the information and assets of the organisation. Training of personnel on online security best practices, such as the avoidance of 'phishing' attacks, with regular and random tests and exercises to ensure compliance with best practices is also recommended.

Monitoring cloud performance

Once security controls have been defined and implemented, the Government Data Manger's team should monitor cloud performance to ensure continued effectiveness. Any government organisation, as a cloud customer, can manage and monitor the effectiveness of their security controls, as long as they have the appropriate policies in place and access to tools from the CSP to do so in in an effective manner. For the customer this means:

1. Being provided with the tools required to securely manage the service;
2. Ensuring that all external or less trusted interfaces of the service be identified and have appropriate protections to defend against attacks through them; and
3. Being provided with the audit records needed to monitor access to their service and the data held within it.

Implementing an effective monitoring framework requires that the relevant roles within the government organisation to be defined as well. Each aspect of **defining, implementing and monitoring** the components of a control framework need to be delegated to specific individuals or teams. Such that it is clear:

- Who is responsible for classifying new data?
- Who is responsible for managing the data?
- Who is responsible for managing access permission?
- Who is responsible for monitoring and reporting on cloud service performance?

The respective individuals and teams should report to, and coordinate their overall approach under, one clearly defined representative in senior management, the Government Data Manager for the organisation. The person or team that is responsible for monitoring cloud performance can then ensure that they have access to the necessary tools and logs from the CSP to monitor aspects of cloud performance such as service availability, network performance, data access and data breaches.

Performance can be compared against the demands of the organisation and reported regularly to the necessary finance, budgeting and evaluation administrators. This will allow cloud ICT resources to be managed and assessed in the same way that other utilities and outsourced services are, and the ICT strategy can be improved over time to match the organisation's need. This can also help the organisation continue to explore new uses of ICT to develop new or better services.

Risk Assessment and Aligning Classifications with types of Security Controls

A risk assessment process has four principal components:

1. Consider **institutional risk**: Risk to personnel, operations, economic loss, national security.
2. Consider **risk of breach**: Desirability of the data to a third party resulting in a heightened risk of external parties seeking the data in questions.
3. **Assign level of risk, High, Medium and Low**, to three criteria: **confidentiality, integrity and availability,** and
4. Determine **appropriate security controls** based on (1), (2) and (3): What are reasonable and appropriate security controls based on the identified risks?

In a cloud-based ICT environment, the risk assessment is done at the point of migrating to the cloud. The cloud customer determines the risks associated with the data that is being migrated to the cloud and classifies the data accordingly with reference to the data classification taxonomy.

Once the data is in the cloud, the cloud customer can monitor the implementation of security controls to determine whether the controls in place are serving their purpose, achieving what they were designed to achieve – and whether the controls that are in place are portable and suitable to be deployed for subsequent use cases.

Determining institutional risk

In assessing security controls, the Government Data Manager first considers the sensitivity of the data, that is, undertaking the data classification process which focuses on institutional risk. Institutional risk is defined by the potential loss that could result from unauthorised access to the data in question. Such as: *Will national security be harmed if the data is* *compromised? Is there a risk that the government or a third party would suffer an economic loss if the data leaked?*

The lack of specificity in the terminology, “limited adverse effect”, “serious adverse effect”, and “severe or catastrophic adverse effect” as categories of impact – illustrates that there is a significant level of subjectivity involved in the institutional risk assessment process.[26] Thus, it is critical that the Government Data Manager is vigilant to avoid over- or under-classification.

Determining risk of breach

Translating institutional risk into security controls requires two further considerations, first, that of the risk of breach and second, the nature of the risk. The risk of breach is based on an assessment of how desirable the data in question would be to unauthorised entities. Desirability of the information to a malicious actor should be evaluated on both the potential for financial or other direct value of the information to a malicious actor, and the potential adverse societal implications (such as harm to businesses, preservation of legal rights, or preservation of political stability). The more desirable the data is, the higher is the risk that unauthorised entities will attempt to access the data – *and the higher the corresponding security measures needed to counteract the risk of unauthorised data access.* **Unauthorised access to personal data or security system controls can lead to huge losses, both for the government, and potentially for third parties as well. This type of data is often of high value (desirability) to the unauthorised person accessing the information.**

Risk of breach is not entirely distinct from institutional risk. Therefore, the Government Data Manager must consider both aspects of risk to determine the appropriate security controls.

Determining appropriate security controls

Risk assessment focuses on the three objectives for security controls**: confidentiality, integrity and availability**.

An individual determining the “Security Category” of GENERAL, SECRET or TOP SECRET for any particular information would subsequently assign a level of potential impact to each, confidentiality, integrity and availability to ascertain the appropriate security controls.[27]

[26] NIST FIPS PUB 199: “Standards for Security Categorisation of Federal Information and Information Systems”. Available at:http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[27] Similarly, one would analyze an information system on the same criteria and assign a Security Category. The intent is to ensure that the information system meets the security requirements for the information on the system. The US government’s **FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems***, in combination with NIST Special Publication 800-53 provide the **security requirements and controls applicable to all federal information and information systems** including HIGH impact information and systems.

- Confidentiality: Confidentiality is the ability to protect information from access by individuals unauthorised to view it.
- Integrity: The ability to ensure that data is an accurate and unchanged representation of the original secure information.
- Availability: The information is readily accessible to the authorised viewer at all times.

One will want to be able to weigh each of the three objectives against a **Level of Impact**: **LOW**, **MODERATE** and **HIGH** and **set a benchmark for security controls for each level.** Here, the goal is to clearly align the need for security with the security measures applied. As an illustration, for LOW, the system would incorporate 100 security controls, MODERATE, 120 security controls and HIGH, 160 security controls. For any given type of information, *confidentiality*, *integrity* and *availability* will be given a Level of Impact (LOW, MODERATE, HIGH) which may give a criteria greater weight in the security analysis. For example, information may score HIGH impact for *confidentiality* and *integrity*, but LOW for *availability*. Thus, the security requirements would weigh toward a larger number of security controls addressing *confidentiality* and *integrity*, and fewer controls ensuring the *availability* of the information.

This system is not unlike those of many large businesses and organisations. A well-run organisation would undertake similar steps to protect its information assets**.** Most government information can be compared to business information; whether it is trade secret or business confidential information, or information core to the operation of the business. So too the range of information security requirements for businesses is similar to that of government. It is up to the government information security specialists to identify those ICT systems that, although designed for the well-run large business, will meet the need of government. As with any well-run large business, the Government Data Manager should task an information security lead organisation to develop guidelines and ensure proper security measures are implemented across the government in a consistent manner.

Risk assessment validation and monitoring

To determine the validity of security controls, the cloud user must have persons or teams in charge of monitoring and assessing the efficacy of the security controls that are in place. A regular practice of reviewing or auditing access to data can reveal breaches or attempted attacks.

To ensure competent validation and monitoring, the cloud user must identify, develop and maintain the skills needed to:

1. Implement and manage ICT resources and service delivery systems on the cloud;
2. Understand, implement, and automate security controls, governance processes, and audits for compliance with security requirements;
3. Define and deploy cloud service monitoring tools and logging systems.[28]

Once the risk assessment has been performed and appropriate security controls have been put in place, the organisation needs a specific set of skills within the organisation to ensure that the risk controls are effective. In-house ICT environments need three distinct skillsets:

1. Professionals that are tasked to ensure the physical security controls, including physical access restrictions, are implemented;
2. ICT professionals that are tasked to ensure that sufficient ICT resources are provisioned to meet the demands of the organisation; and
3. Professionals that know how to operate the logical controls for data access, software-based security controls and performance monitoring.

Effective risk controls in a cloud-based ICT environment depends on a different set of skills than what is needed in a traditional, in-house ICT environment. Since physical security controls are outsourced to the CSP, the cloud customer needs professionals that can negotiate and manage cloud services on the procurement level and on the service management level. These may include:

1. Legal counsel, with input from engineers and developers, that are tasked with negotiating and managing cloud SLAs. SLAs set out the ICT service commitments from the CSP to the cloud customer, so the cloud customer must have the skills needed to ensure the services will meet their demand.
2. Professionals staff to monitor and review cloud compliance audits. This may include internal personnel or professional audit agencies. Audit agencies such as e.g. British Standards Institution (BSI) provide audit services for CSPs' compliance with ISO cloud security standards; the cloud customer should request and review such audit statements from their service providers.
3. System operators and engineers to design the control framework, manage access permissions, monitor the operation of security controls, and assess the portability of security controls from one application to another.
4. Developers, typically working together with system operators and engineers, can help cloud customers that seek to develop a "DevOps" culture. A DevOps culture in

[28] Amended from AWS DevOps Engineer exam concepts:http://aws.amazon.com/certification/certified-devops-engineer-professional/

an organisation is characterised by continual exploration and development of new operations that can automate, enhance or otherwise improve the organisations' service delivery. With the flexible ICT environment provided by the cloud, system operators and engineers have access to the tools needed to explore such new solutions on a continual basis through developing and testing new cloud applications and services.

Fostering Openness through an Open Data Policy (A5)

With the aim of improving governance, building trust and transparency, the Myanmar Government will establish an Open Data policy (A5) to solidify its efforts in open government data.

Introduction

Open data is digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere.[29]

Data is a valuable national resource and asset of the Myanmar Government. To ensure that the Government is taking full advantage of its information resources, individual ministries and agencies must manage data in a way that promotes openness and interoperability. This shall increase efficiencies, reduce costs, improve service delivery, protect personal information, and increase public access to valuable government information.

There are numerous benefits identified from making data resources accessible, discoverable, and usable by the public. From the economic perspective, it can help fuel entrepreneurship and innovation, stimulate foreign investment and create new opportunities for economic development.

This policy details one consistent approach to the sharing of data held by all government ministries, agencies and departments of government (hereafter referred to as "agencies"). Furthermore, it shall represent the Myanmar Government's position and approach on how data resources are to be treated. Whether or not particular information can be brought in the public domain, agencies can apply the requirements laid in this policy to all data resources to promote efficiency and produce value.

[29] International Open Data Charter

Specifically, this policy requires all agencies to collect or create data in a way that supports processing and dissemination at later stages. This includes using machine readable and open formats and data standards for all new data. It also includes agencies to ensure data stewardship through use of open licenses and review of data for privacy, confidentiality, security or other restrictions. In addition, it necessitates that all agencies build or modernise information systems to maximise interoperability and accessibility, maintain data inventories, continue to enhance defences and clearly define information management responsibilities.

The Myanmar Government has already made significant progress in improving its management of data resources to increase interoperability and openness. All agencies have been instructed to take actions to implement the principles of transparency and collaboration and expand access to information. In addition, this policy outlines the plan to populate a robust National Open Data Portal with data already collected and that which will be created in the future. This online platform will be designed to increase access to government data. The publication of data through the portal will continue to benefit the public and produce economic development opportunities.

Definition of Terms

This section provides definitions as well as principles that an open data policy should be consistent with.

- **Data**: For the purposes of this document, all structured information, unless otherwise noted
- **Dataset**: For the purposes of this document, a collection of data presented in tabular or non-tabular form
- **High-value dataset**: Datasets which are useful to a large audience or brings large value to a specific target audience; have high use and re-use potential; and re-use has strong potential social and economic impact.
- **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.
- **Open**: Refers to software, data and other content provided electronically, being freely accessible for use and reuse, for sharing for any purpose (without restrictions save for the necessary to preserve openness).

- **Open data**: For the purposes of this document, digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere. In general, it shall be consistent with the following principles:

1. The data held by agencies or organisations on behalf of these public bodies, are public assets held by the Government on behalf of the people.
2. The value of data as a public asset must be maximised, with access that ensures that use of data is not mutually exclusive.
3. Government to adopt a presumption in favour of openness to the extent permitted by law and subject to privacy, confidentiality and security restrictions.
4. Data to be made available in a timely manner, without waiting for specific requests. Government to also respond positively to additional requests for data.
5. Data to be available at the marginal cost of distribution, and free of charge over the internet.
6. Data to be available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed and searched. Formats should be machine-readable. To the extent possible, these formats should be non-proprietary, publicly available and no restrictions be placed on their use.
7. Data to be re-usable for any lawful purpose, commercial or non-commercial.
8. In addition to releasing its own data, Government of Myanmar will encourage and facilitate the release of data by other state and local governments, private sector and civil society.
9. The Government will promote the use of its open data and ensure that it provides maximum benefit to citizens and society.
10. A point of contact will be established to assist with data used and respond to complaints and feedback about adherence to these open data requirements.

Open Data Portal

The Open Data Portal will be established by the ITCSD. It will be a single, authoritative platform for the Government, and linked to the Myanmar National Portal. A single platform for all data of the government will make it fast and efficient for users to find the required information.

Individual agencies will not need to develop their own Open Data portals and should not do so. They should focus on releasing their data in a timely manner, providing it and its metadata in open formats and working with users of the data.

The next section details the requirements of agencies in the management of information resources.

Policy Requirements

The requirements in this section, part 1 and 2, apply to all new data collection, creation, and system development efforts, as well as projects that modernise existing information systems. The requirements in part 3 apply to the management of all datasets used in an agency's information systems. All agencies are encouraged to improve the accessibility and usability of their existing datasets by making them 'open' using the methods outlined in this policy, prioritising high-value datasets.

All government agencies shall take the following actions to improve the management of data resources and reinforce the government's presumption in favour of openness:

1.Collect or create data in a way that supports its processing and dissemination. Specifically, the agencies should:

a. Use machine-readable and open formats: While information should be collected electronically by default, machine-readable and open formats must be used in conjunction with both electronic and telephone or paper-based information collection efforts. To the extent permitted by law, the use of open formats that are non-proprietary and publicly available should be used.

b. Use data standards: Consistent standards and guidelines for data will be developed. They will be used for data as it is collected or created, and agencies must use them to promote data interoperability and openness. Publishing of individual datasets that do not fully conform to the necessary standards may be permitted where the early availability of the dataset in non-compliant form would nevertheless be valuable to the users of that data. However, any deviation from standards should be explained and an agreed timeline to conform to standards must be set.

c. Apply open licenses: Open licenses must be applied to information collected or created, so that data made public has no restrictions on copying, publishing, distributing, or any other usage for commercial or non-commercial purposes.

d. Publish metadata: Metadata associated with each data set to be published. It should include information about origin, linked data, geographic location, data quality, and other relevant indices that reveal relationships between datasets and allow the public to determine the fitness of the data source. The common metadata may also be expanded based on standards, specifications, or formats developed within different sectors (financial, health, law enforcement).

2. Build or modernise information systems that support interoperability and information accessibility. The system design must be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design.

3. Strengthen data management and release practices. Within six months of the date of this policy, agencies are to review and where appropriate revise existing policies and procedures to strengthen their data management and release practices. While ensuring consistency with the requirements of this policy, they should take the following actions:

a. Create and maintain an enterprise data inventory. All government agencies should build an enterprise data inventory, that accounts for datasets used in the agency's information system. The inventory will indicate all datasets, which of these may be made public and whether they are currently available to the public.

b. Create and maintain a public data listing. All datasets in the enterprise data inventory that can be made public must be listed on the official website of the agency in a human-and-machine readable format. This should then enable automatic aggregation by the national portal. Over time, this should include all agency datasets that can be made publicly available.

c. Engage with customers to facilitate data release. Engagement with customers is necessary to prioritise the release of datasets and determine the most appropriate formats for release. For instance, high-volume datasets that may be of interest to developers should be released using bulk downloads as well as Application Programming Interfaces (APIs).

d. Clarify roles and responsibilities for efficient data release practices. All government agencies should ensure that roles and responsibilities are clearly designated for the promotion of efficient data release practices. These include:

    i. Communicating the strategic value of open data to internal stakeholders and the public
    ii. Ensuring that data released is open, with a point of contact established to respond to complaints or feedback
    iii. Encourage businesses and the civil society to use the data to build applications and services
    iv. Scale best practices from bureaus or offices that have superior open data practices
    v. Work with other stakeholders to ensure that privacy and confidentiality are not compromised
    vi. Work with the security teams to assess risks of releasing potentially sensitive data and security safeguards in place.

4. Reinforce measures that guarantee privacy, confidentiality and security of all data. All data collected or created should be analysed to check whether it can be made public, consistent with the presumption in favour of openness, and to the extent permitted by law and subject to privacy and security restrictions. If it cannot be made publicly available, the agency should document these reasons.

5. Incorporate interoperability and openness requirements into all data management processes. All agencies should integrate data management activities into their core processes of organisational planning, budgeting, procurement and financial management. They must also institutionalise the requirements of interoperability and openness, mentioned in this policy, in all their processes.

Implementation

This section delineates key features of the overall implementation of the policy, as well as elements specific to agencies.

1. **Roles and responsibilities:**

   Central Team: A central team will be constituted, consisting of core agencies to ensure that the necessary structures are in place for a well-functioning Open Data Portal. The ITCSD will chair this central team and coordinate all activities of the team. It may comprise of representatives from the following agencies:

   a. Central Statistical Organisation, Ministry of Planning and Finance
   b. Ministry of Information
   c. Other selected agencies with large, high value datasets

   The central team will be responsible for:

   a. Overall Open Data policy
   b. Producing detailed guidance to all agencies and department on Open Data implementation
   c. Setting business and technical standards for Open Data
   d. Overall programme definition and programme management
   e. Implementation strategy and prioritisation
   f. Establishing skill development programmes inside and outside government
   g. Ensure requests for data are being properly considered by the relevant agencies, and work with them to see how they can be met.

h. Development and operation of the Open Data portal
i. Establishing and enforcing standards for metadata associated to datasets in the open data portal
j. Helping with data release decisions and preparations, including privacy and security assessments, anonymisation and other necessary work.

To implement this policy, all agencies should strategize and first implement those elements that can be addressed earliest or support critical objectives. Their main, permanent responsibilities are:

a. Release of data as authorised by the respective agency head, or by someone who is given authority to do so.
b. Appointment of a contact person in the agency, who will liaison with the central team and ensure that the necessary data releases are done.
c. Ensure that all agreed data releases are done, and any issues or difficulties are reported to the central team.
d. Sharing and submission of the enterprise data inventory.

2. Resources:

Policy implementation will require investment, depending on the existing data management processes of the agencies. They are encouraged to evaluate current processes and identify implementation opportunities that result in the most efficient use of public money. The potential investments, tools and resources needed to meet these policy requirements should be funded through their capital planning and budget processes.

3. Measurement and review:

The central team will develop a measurement and reporting framework to measure progress on the requirements laid down in this policy. Periodic measurements will also be made of the Open Data portal, including number of visitors, number of datasets, number and category of downloads of datasets, number of agencies contributing data to the portal, API usage, number of entrepreneurs, businesses or developers registered, number of requests for data received, feedback and other community activity.

This policy will be regularly reviewed, in the light of experience and comments received from agencies, as well as data users.

Part II: Policies Related to E-Commerce

Background

This is the National e-Commerce Policy which accompanies the set-up of the E-Commerce Steering Committee (see Myanmar Cyber Law, Part IV). The committee should act as the lead public sector agency in facilitating electronic commerce in Myanmar. Having this body will allow for the creation of a legal, regulatory and policy environment conducive to the development and use of electronic commerce. It will further enable Myanmar to utilise information and communication technologies to drive economic growth and social development.

Due to the cross-cutting nature of e-Commerce issues, two components of the cyber security category are covered in this policy, namely C3 E-Authentication, and C4 E-Signatures. For the same reason, it is recommended that the E-Commerce Steering Committee align its work with the following groups:

1. e-Government Steering Committee,
2. e-ID Working Committee,
3. Consumer Protection Central Committee (CPCC)
4. Digital Economy Development Committee
5. Ministry of Labour, Immigration and Population
6. Consumer Protection Department, Ministry of Commerce
7. Customs Department, Ministry of Planning and Finance
8. Central Bank of Myanmar.

Cross Border Transfer of Information by Electronic Means (B1)

1. The committee will promote the safe and secure flow of data across borders in the context of e-Commerce and online trade.
2. Enabling Cloud Computing: The committee will promote the use of cloud computing in the public sector (see Cloud First Policy.)
3. International Consistency
    a. The committee will ensure that cross border data flows policies are aligned with global norms, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).
    b. The committee will define strong data protection laws which balance the protection of consumer data with the need for allowing the data to flow across borders.

    c. The committee will work with the Consumer Protection Department of the Ministry of Commerce, the Consumer Protection Central Committee, and the Personal Data Privacy Commission to develop strong data protection law.

4. Cross Border Movement of Data
    a. The committee will ensure there are no restrictions on where data can reside.
    b. To streamline the process of data compliance, the committee should implement a policy on Data Classification (see above).
    c. The committee should ensure there is no discrimination between local and foreign cloud and data service providers.
5. Regulatory Stability and Enforcement
    a. The committee will ensure that it is easy to set up online businesses with minimal requirements and licensing.
    b. The committee will ensure that Myanmar aligns its cross border data flow policies with international and regional frameworks, such as:
        i. ASEAN Framework on Digital Data Governance[30], in particular Strategic Priority 2, on ASEAN Cross Border Data Flow Mechanism,
        ii. APEC Cross Border Privacy Rules (CBPR) system.[31]

Electronic Settlement (B2)

1. To increase access and interoperability of banking services, the committee should work with the financial services industry and the Central Bank of Myanmar to increase the number of individuals aged 15+ who have a bank account (including mobile money account).
2. The committee should work with the financial services industry, and the Central Bank of Myanmar, to accelerate the rollout and adoption of interbank payment mechanisms, such as payment switches.
3. The committee should work with the financial services industry, and the Central Bank of Myanmar, to remove any limitations on interbank payments and transfers.
4. Review and Update of Banking Regulations - The committee should establish a work project to develop a comprehensive e-Commerce regulation in collaboration with the stakeholders in the financial services industry.

Paperless Trading (B3)

1. Government Adoption of Paperless Notifications and e-Payments

[30] https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf
[31] http://cbprs.org

a. The committee should ensure all government agencies are able to adopt e-payments in all their transactions, such as with other government agencies (e.g. inter-agency payments), private businesses (e.g. licence payments and permits), and citizens (e.g. licenses, tax, collection of tolls, social security disbursements.)
b. The committee should ensure all government agencies are able to adopt paperless and digital notifications e.g. notifications via email, mobile notifications.
c. The committee should work with the e-Government Steering Committee, to align efforts to the National ICT Strategy, especially regarding standardizing the ICT approach towards government adoption of technology and a cloud first policy. Issues related to e-Commerce would include enabling interoperable standards for issuing invoices, receiving payments, selecting cloud infrastructure, software, maintenance, and other e-Government standards.
d. The committee should also align paperless trading policies with international and regional frameworks, such as the ASEAN Agreement on e-Commerce.

2. The committee should develop, enable, and accelerate work in the following areas:
   a. Fully implement the automated e-customs system (Myanmar Automated Cargo Clearance System (MACCS), in collaboration with the Customs Department,
   b. Ensure internet connection is available to customs and other trade control agencies at border crossings,
   c. Develop Myanmar’s National Single Window (NSW) to join the ASEAN Single Window (ASW) system,
   d. Allow for electronic submissions of customs declarations,
   e. Enable electronic application and issuance of preferential certificates of origin, and Sanitary and Phytosanitary Certificates, and enabling electronic exchange of these certificates with other countries,
   f. Allow for electronic application for custom refunds,
   g. Establish recognised certification authority to issue digital certificates to traders to conduct electronic transactions,
   h. Engage in trade-related electronic data exchange with other countries, such as allowing for electronic tracking of shipments by the Customs Department,
   i. Allow banks and insurers to retrieve letters of credit electronically without lodging paper-based documents.

Custom Duties (B4)

1. The committee should work with the Ministry of Planning and Finance to develop the electronic payment of customs and other related e-Commerce taxes. This is being planned in a new e-customs law.
2. The committee should work with the Ministry of Planning and Finance on a tax collection plan for online businesses.
3. The committee should work to introduce an electronic system for payment of customs duties and refunds (see B3 Paperless Trading).

Online Trade (B5)

1. The committee should work to encourage internet penetration in the country, in tandem with the Universal Service Obligation Fund (see e-Government section on Building Information Infrastructure).
2. The committee should work to improve business-to-consumer web presences in the country, such as increasing the number of secure internet servers per 1 million people in the country.
3. Dispute Resolution Mechanism - The committee should work with the Consumer Protection Central Committee to ensure that the dispute resolution mechanism provided for in the Consumer Protection Law (consumer dispute settlement bodies) works smoothly and effectively for e-Commerce transactions.

E-Authentication (C3)

1. The committee should work with the e-Government Steering Committee, Union Auditor General's Office, the Ministry of Labour, Immigration and Population, the e-Government Steering Committee, and the e-ID Working Committee to update regulations and legislation regarding digital identities, authentication methods, and digital signatures.
2. E-Authentication
    a. Security Standards: The committee should work with the e-Government Steering committee, the Central Bank, and the Union Auditor General's Office to establish strong e-authentication and e-payments security standards and guidelines for both the government and private sectors, such as:
        i. Ensuring secure connections via HTTPS,
        ii. Supporting international standards for added security, such as EMV (EuroPay, Mastercard, Visa), and Payment Card Industry Data Security Standard (PCI DSS),

        iii. Setting up a National Certification Authority (National CA) under the National Cyber Security Centre, to govern digital authorisations and enable secure mobile payments.

3. E-Identity
    a. The committee should work with the Ministry of Labour, Immigration and Population and the e-ID Working Committee to accelerate the issuance of identity cards and unique identity numbers to all Myanmar citizens and residents.
    b. The committee should also establish a government policy endorsing the use of these unique numbers as a government standard for verifying Myanmar citizen identity.
    c. The committee will work with the Personal Data Protection Commission, and the Consumer Protection Department of the Ministry of Commerce, to ensure that personal data is adequately protected, and prevent any potential identity misuse.

E-Signatures (C4)

1. The committee should ensure that both the Electronic Transactions Law is amended and aligned with Articles 9, 12(2), 12(3) of the UNCITRAL Model Law on Electronic Signatures, which recognises the validity of electronic and digital signatures. (See Myanmar Cyber Law, Part IV.)
2. The committee will ensure that the Evidence Act is amended to incorporate Article 6(3) of the UNCITRAL Model Law on Electronic Signatures, which recognises the legal validity and reliability of digital signatures. (See Myanmar Cyber Law, Part IV.)

Part III: Policies Related to Cyber Security

Introduction

The Myanmar Cyber Law addresses Cybersecurity in Chapter (V), sets up a Personal Data Protection Commission (PDPC) in Chapter (VI), and also provides the legislative foundation for Computer Misuse and Cybercrime in Chapter (VII). To address the cyber security needs of Myanmar (see Chapter (V) of the Draft Law) two policies[32] are recommended:

1. Establishing a Personal Data Protection Commission to address C1 Privacy and Data Protection; and
2. Establishing a National Cybersecurity Strategy to address C2 Reducing Exposure to Cyber Threats and Cybercrimes.

Privacy and Data Protection (C1) through the Personal Data Protection Commission

1. Establishment of the Personal Data Protection Commission
    a. The Myanmar Cyber Law will establish the Personal Data Protection Commission (PDPC). As the PDPC is being established, the following measures should be undertaken to ensure international best practices (see Policy Benchmarking Report.)
    b. The Myanmar PDPC should be established as an effective agency or regulator which is tasked with the enforcement of privacy laws.
2. Myanmar should update the existing 2017 Law Protecting the Privacy and Security of Citizens – or, alternatively, have the Personal Data Protection Commission issue data protection rules by notification – to include online data, and establish rules governing the collection, use, or other processing of personal information.
3. This update should define core privacy and data concepts:
    a. Personal Data - Personal data refers to any information that is related to an identified or identifiable natural person. Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law.
    b. Personally identifiable information (PII) - PII refers to any data that can be used on its own or with other information to distinguish one person from another; to identify, contact, or locate a single person; or to identify an individual in context. This includes identification numbers (e.g. social security number) or one or more factors specific to physical, physiological, mental,

[32] C3 (Electronic authentication) and C4 (Electronic signatures) are covered in the e-Commerce Policy.

economic, cultural, or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA, etc.).

c. Data Owners - A data owner is a person who is accountable for a data asset. Within organisations, data ownership typically goes to a department, team, or business unit that can authorise or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.
d. Data Controllers - A data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed.
e. Data Processors - A data processor is a person (other than an employee of the data controller) who processes the data on behalf of the data controller.
f. Data Processing - Data processing means obtaining, recording, or holding data, as well as carrying out any operation or set of operations on the information. This includes:
    i. organisation, adaptation, or alteration of the information or data;
    ii. retrieval, consultation, or use of the information or data;
    iii. disclosure of the information or data by transmission, dissemination, or otherwise making available;
    iv. alignment, combination, blocking, erasure, or destruction of the information or data.
g. Data classification types such as open data and public data (See Data Classification Framework and Open Data Policy in National ICT Strategic Plan)

4. This update should also allow Myanmar to adhere to the requirements for inclusion in the APEC Privacy Framework, and the EU's General Data Protection Regulation (GDPR).
5. This update should clarify registration guidelines around data controllers - organisations could develop policies and practices to designate at least one data controller to oversee personal and organisational data protection responsibilities. To maximise compliance, organisations could ensure data controllers are registered with government entities in charge of data privacy protection. This registration process could be modelled on Singapore's Personal Data Protection Commission (PDPC).
6. This update should also include a breach notification requirement. A data breach occurs when personal data and/or PII held by an organisation is lost or subjected to unauthorised access or disclosure. For instance, the EU's GDPR mandates that all notifications of data breaches must be submitted within 72 hours of the its occurrence. Organisations could be required to notify affected individuals and the

relevant government authority when a data breach is likely to result in serious harm to individuals whose personal information is involved in a breach. For instance, the EU GDPR mandates that all data that can "result in a risk for the rights and freedoms of individuals" should be reported within 72 hours of first having become aware of the breach.[33]Notifications to affected individuals would include recommendations about the steps individuals should take in response to the breach. Additional breach notification provisions could be modelled on Australia's Notifiable Data Breaches (NDB) scheme, which the Office of the Australian Information Commissioner (OAIC) introduced under the Privacy Act 1988 in February 2018.[34]

7. The update should promote cross border transfer of data. Cross-border provisions could be included to ensure organisations are able to move data freely to whichever physical or virtual location they are needed. The transfer of personal data to recipients outside Myanmar would be allowed in the following cases:
    a. the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
    b. the data exporter puts in place appropriate safeguards; or
    c. an exemption applies.

[33] https://eugdpr.org/the-regulation/

[34] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Exposure to Cyber Threat and Cybercrime (C2) with a National Strategy for Cybersecurity

In order to decrease the incidence of cyber threats and reduce Myanmar citizens' exposure to cybercrime, it is important to establish a National Strategy for Cybersecurity.

Roles and Responsibilities

1. The National Strategy for Cybersecurity will be led by the ITCSD, as noted in the Myanmar Cyber Law.
    a. Due to the cross-cutting issues involved with cybersecurity, the ITCSD should in particular work with the following groups, apart from other relevant departments within the Ministry of Transport and Communications:
        i. Ministry of Office of the President
        ii. Ministry of Home Affairs (in particular, the Myanmar Police Force)
        iii. Ministry of Defence
        iv. Union Attorney General's Office
        v. Private sector organisations as required.
    b. It is recommended that the National Strategy for Cybersecurity be reviewed periodically with public consultation.
    c. It is recommended that the National Strategy for Cybersecurity be assessed against international metrics (such as the ITU's Global Cybersecurity Index) to ensure international standards and compatibility.
    d. In response to the observation that there is little clarity around which government agency has the primary responsibility and right to respond to cybersecurity threats and cybercrime, it is recommended that the ITCSD work with all stakeholders to establish clear roles and responsibilities in the government, and communicate this to the general public. This will ensure that the government improves response times to cyber threats and cybercrimes.

Protection of Critical Information Infrastructure (CII)

1. Definition of CII: A computer or computer system can be defined as CII, if:
    a. the computer system it is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system would have a debilitating effect on the availability of the essential service in the Republic of the Union of Myanmar; and
    b. the computer or computer system is located wholly or partly in the Republic of the Union of Myanmar.

2. Determining CII: The ITCSD should obtain information from owners of computer systems to ascertain whether these systems fulfil the criteria for CII, in the event that there is reason to believe that a particular system is to be designated as a critical information infrastructure. The ITCSD is also empowered to determine when a system no longer fulfils the criteria of a critical information infrastructure, and may be withdrawn from being designated as a CII.
3. Control, Governance, and Compliance Mechanisms for CII: the ITCSD may
    a. Request additional information from the owner of a critical information infrastructure on the design, configuration and security;
    b. Develop and issue codes of practice and standards of performance for the regulation of owners of critical information infrastructures to ensure cybersecurity of these systems,
    c. Introduce requirements for owners of CII to report any cybersecurity related incidents on a computer system under the owner's control, including computer systems that are interconnected with or communicate with critical information infrastructure,
    d. Mandate the owner of CII to conduct regular cybersecurity audits and risk assessments of the critical information infrastructure.

Cybersecurity Risk Assessments, Controls, and Audits

1. The Myanmar Cyber Law sets out the functions and responsibilities of mmCERT, which includes cybersecurity risk assessments, monitoring, and control mechanisms.
2. mmCERT and ITCSD should work to ensure a strong incident reporting culture of cyber attacks so that digital forensic analysis may be performed, and cyber attack trends identified. For example, the Netherlands compiles disclosure reports, security advisories and incidents using a registration system, on an annual basis. This is reported in their Cyber Security Assessment Netherlands Report[35], which alerts cybersecurity professionals to act on emerging threats.
3. Cybersecurity assessments, controls, and audits should adhere to international standards (see Standards section in the National ICT Strategy). Independent audits may therefore be conducted using these control mechanisms.

Cybercrime

1. Chapter VII on Computer Misuse and Cybercrime of the Draft Cyber Law establishes a Cybercrime Working Committee to act as a lead agency to promote awareness of

[35] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

cybercrimes and develop legislative and other measures to protect the integrity of data and computer systems.

2. The Cybercrime Working Committee should focus on the following roles and responsibilities:
    a. Work with the National Cyber Security Centre and mmCERT to raise awareness about cybersecurity risks,
    b. Work with the e-Government Steering Committee to develop training programmes for cybersecurity professionals, especially for mmCERT personnel, to adequately respond to cyber threats. Myanmar can look to learn from the efforts other countries have taken to adequately prepare for cyber threats. For instance, Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training via higher education institutions in Malaysia,
    c. Review and propose updates to various criminal laws to include online crimes and other types of cybercrimes as proposed in the Myanmar Cyber Law
    d. Work with the public and private sectors to address cyber threats
        i. To adequately respond to cyber threats, the Cybercrime Working Committee should also focus its efforts on enhancing coordination between the public and private sectors.
        ii. Myanmar could also consider engaging in bilateral and multilateral agreements for cooperation on cybersecurity, which could include Mutual Legal Assistance Treaties (MLATs), and other collaborative initiatives through ASEAN, APEC, Council of Europe etc.
        iii. Myanmar can actively participate in bilateral and multilateral engagements with regional and international CERTS. Myanmar could also look to set-up sectoral CERTs such as FinCERT, ISP/Telecom CERT, CII Operator CERT and Academic CERT and facilitate cooperation between the National CERT (mmCERT) and sectoral CERTs.

Lawful Intercept

1. The Cybercrime Working Committee should work with the e-Commerce Steering Committee, Digital Crimes Department of the Myanmar Police Force, as well as the Post and Telecommunications Department (PTD), to implement a transparent mechanism for obtaining access to data via a court warrant or similar process that is based on proper due diligence, reasonable frequency of request, and ability for the

relevant parties to adhere to or challenge the data request. (see also Enabling Data Safety section in the e-Commerce Policy.)

2. As this is a cross-cutting issue which overlaps substantially with the role of an independent telecommunications regulator, the Cybercrime Working Committee may wish to discuss and assign clear roles and responsibilities in initial discussions with the e-Commerce Steering Committee, the Myanmar Police Force, as well as the PTD.
3. It is also recommended that a broad public consultation be conducted on any lawful intercept mechanism proposed.

Spam

1. The Cybercrime Working Committee should formulate national policies related to the containment or curbing of online spam and continue to provide guidance documents and recommendations to upgrade Myanmar's level of protection against cyber threats through firewalls, security licenses and certificate renewals, to keep up with the growing sophistication of online crimes.
2. The Cybercrime Working Committee could consider extending Myanmar's capacity to undertake digital forensics beyond what is being carried out by the Cyber Crime Division (CID) of the Myanmar Police Force (MPF), by bringing in government accredited third party providers to carry out digital forensics for non-police cases.