MALAYSIA MADANI

MINISTRY OF DIGITAL
MALAYSIA

NATIONAL CLOUD COMPUTING POLICY

MADANI : Secure, Sovereign, Inclusive, and Sustainable Cloud Futures

PUBLISHED BY

MINISTRY OF DIGITAL

Aras 13, 14 & 15, Blok Menara,
Menara Usahawan
No. 18, Persiaran Perdana, Presint 2
Pusat Pentadbiran Kerajaan Persekutuan
62000 Putrajaya, Malaysia

Tel : **+603-8000 8000**
Email : **pengupayaan@digital.gov.my**
Instagram : **www.instagram.com/kementeriandigitalmalaysia**
Facebook : **www.facebook.com/KementerianDigitalMalaysia**
X : **x.com/KemDigitalMsia**
Tiktok : **www.tiktok.com/@kementeriandigital**

PREFACE - NATIONAL CLOUD POLICY

YB TUAN GOBIND SINGH DEO
Minister of Digital Malaysia

The digital era has transformed the global landscape, ushering in unprecedented opportunities for innovation, efficiency, and inclusivity. Cloud computing stands at the heart of this transformation, providing a scalable, resilient, and cost-effective infrastructure that empowers governments, businesses, and individuals to thrive in an interconnected world.

Malaysia recognises the transformative potential of cloud computing in driving our nation's progress and strengthening our digital economy. As part of our commitment to achieving the aspirations of MyDIGITAL and the Malaysia Digital Economy Blueprint, this National Cloud Computing Policy serves as a strategic guide to harnessing cloud technology responsibly and effectively.

This policy outlines a comprehensive framework for promoting cloud adoption across sectors while ensuring robust security, privacy, and governance safeguards. It reflects our unwavering dedication to fostering a vibrant digital ecosystem that supports economic growth, enhances public service delivery, and improves the quality of life of all Malaysians.

The journey towards becoming a leading digital nation requires collaboration and a shared vision. I extend my gratitude to all stakeholders, including government agencies, industry leaders, academia, and civil society members who have contributed to the development of this policy. Together, we can build a future where technology serves as an enabler of inclusive and sustainable progress.

As we implement this policy, I urge all Malaysians to embrace the opportunities that cloud computing offers. Let us work collectively to unlock its potential, address challenges, and position Malaysia as a global leader in digital innovation.

GOBIND SINGH DEO
Minister of Digital
Malaysia

MESSAGE BY SECRETARY- GENERAL MINISTRY OF DIGITAL

YBHG. TUAN FABIAN BIGAR
Secretary-General Ministry of Digital Malaysia

The digital era offers unparalleled opportunities for transformation, innovation, and inclusivity. At the heart of this transformation lies cloud computing, a pivotal technology that enables governments, businesses, and communities to unlock their full potential in an increasingly interconnected world.

Malaysia's commitment to embracing the digital revolution is evident through the aspirations of the MyDIGITAL initiative, the Malaysia Digital Economy Blueprint and National Fourth Industrial Revolution Policy. As we advance towards these national goals, the National Cloud Computing Policy serves as a strategic roadmap to ensure the responsible, secure, and efficient adoption of cloud technologies across all sectors.

This policy aims to establish a robust cloud ecosystem that accelerates the delivery of public services, fosters innovation, and strengthens the nation's economic resilience. It provides a framework to address critical aspects such as security, data sovereignty, and accessibility, ensuring that cloud adoption aligns with our nation's values and priorities.

The development of this policy reflects the collaborative efforts of government agencies, industry leaders, and stakeholders who share a vision of a digitally empowered Malaysia. Together, we have crafted a policy that not only addresses the challenges of today but also anticipates the demands of tomorrow.

As we embark on this transformative journey, I urge all stakeholders to actively engage with the principles and guidelines outlined in this policy. By leveraging the power of cloud computing, we can drive meaningful progress and position Malaysia as a leader in the global digital economy.

Let us work together to build a resilient, inclusive, and innovative digital future for all Malaysians.

FABIAN BIGAR
Secretary-General Ministry of Digital Malaysia

ACKNOWLEDGEMENT

The formulation of the National Cloud Computing Policy would not have been possible without the dedication, collaboration, and commitment of various stakeholders who have contributed their expertise, time, and insights :

Ministry of Digital

- The Office of Secretary General
- The Office of The Deputy Secretary-General (Digital Development)
- The Office of The Deputy Secretary-General (Strategic & Management)

Ministry of Digital Department And Agencies

Department :
-National Digital Department (JDN)
-Personal Data Protection Department (JPDP)

Agencies :
-Malaysia Digital Economy Corporation (MDEC)
-MyDigital Corporation (MyDIGITAL)
-CyberSecurity Malaysia (CSM)
-Digital National Berhad (DNB)
-Malaysian Network Information Centre (MYNIC)

Ministries

- Ministry of Education
- Ministry of Higher Education
- Ministry of Health
- Ministry of Transport
- Ministry of Communication
- Ministry of Science, Technology and Innovation
- Ministry of Investment, Trade and Industry
- Ministry of Natural Resources and Environmental Sustainability
- Ministry of Energy Transition and Water Transformation
- Ministry of Economy

Government Agencies

- National Cyber Security Agency (NACSA)
- Malaysia Office of the Chief Government Security Officer (CGSO)
- Prime Minister's Department (JPM)
- Malaysian Communications And Multimedia Commission (MCMC)
- Central Bank of Malaysia (BNM)

Industry Associations & Players

- Microsoft Malaysia
- Google Malaysia
- Telekom Malaysia
- Amazon Web Services
- Enfrasys Consulting Sdn Bhd
- Radmik Solutions Sdn Bhd
- Awantec Systems Sdn Bhd
- Cloud Connect Sdn Bhd

Key Collaborator

Futurise Sdn Bhd

TABLE OF CONTENT

GLOSSARY

Key Terms and Definitions

To assist readers in understanding the technical terminology used throughout the NCCP, a glossary of key terms is provided:

TERM	DEFINITION
Artificial Intelligence (AI) in Cloud	The integration of AI tools and capabilities into cloud computing environments to enhance data processing, automation, and service delivery.
Artificial Intelligence (AI)	The simulation of human intelligence processes by machines, especially computer systems.
Cloud Computing	A model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., servers, storage, applications) that can be rapidly provisioned and released with minimal management effort.
Cloud Deployment Models	The methods by which cloud services are deployed, including public, private, hybrid, multi and community clouds.
Cloud Security	The policies, controls, and technologies that protect cloud-based systems, data, and infrastructure from threats.
Cloud Certification	Accreditation or certification programs that validate the security, compliance, or quality standards of cloud services.
Cloud Migration	The process of transferring data, applications, or other business elements to a cloud environment.
Cloud Governance	The framework for decision-making and accountability regarding the use of cloud computing in an organisation or nation
CyberSecurity Malaysia	A company limited by guarantee which provides cyber security services
Cloud Service Provider (CSP)	A company or organisation that offers cloud computing services.
Cloud Readiness	The level of preparedness of an organisation or nation to adopt cloud computing technologies effectively.
Cloud Migration	The process of transferring data, applications, or other business elements to a cloud environment.
Data Privacy	The protection of personal and sensitive data from unauthorised access and ensuring compliance with data protection laws.

TERM	DEFINITION
Data Residency	The physical or geographical location of an organisation's data or information.
Digital Economy	An economy primarily based on digital technologies, including e-commerce, online platforms, and cloud computing.
Data Sovereignty	The concept that data is subject to the laws and governance structures within the nation where it is collected or processed.
Digital Transformation	The integration of digital technology into all areas of a business or government, fundamentally changing how they operate and deliver value.
Green Cloud Computing	Practices that aim to achieve energy efficiency and reduce the environmental impact of cloud infrastructure.
Interoperability	The ability of different cloud systems or organisations to work together seamlessly, enabling data sharing and application portability.
Internet of Things (IoT) in Cloud	The connection and management of IoT devices and data streams through cloud platforms to enable real-time monitoring and analytics.
Malaysia Digital Economic Blueprint (MYDIGITAL)	A strategic initiative introduced by the Malaysian government to accelerate the nation's transformation into a digitally-driven, high-income economy.
Micro, Small, and Medium Enterprises (MSME)	A business entity in Malaysia is classified as an MSME based on either its annual sales turnover or the number of full-time employees, whichever is lower.
Malaysia Digital Economy Corporation (MDEC)	The government agency responsible for driving the development of Malaysia's digital economy.
New Industrial Master Plan 2030 (NIMP 2030)	Comprehensive blueprint designed to elevate Malaysia's manufacturing sector to new heights.
National Institute of Standards and Technology (NIST)	U.S. government agency that promotes American innovation and industry by advancing measurement science, standards, and technology.
RMK 13	Refers to the 13th Malaysia Plan, a comprehensive development plan for Malaysia that outlines the government's strategies and priorities for the period 2026-2030.

TERM	DEFINITION
Service Level Agreement (SLA)	A formal agreement between a cloud service provider and a user that outlines the level of service expected, including uptime, performance, and issue resolution timelines.
Sovereign Cloud	Refers to a cloud computing infrastructure designed to ensure that data is stored, processed, and managed within the legal jurisdiction and governance framework of a specific country.
Small and Medium Enterprises	Small and Medium Enterprises (SMEs) are businesses defined by annual sales turnover and number of full-time employees, categorised as Micro, Small, or Medium Enterprises based on thresholds set by SME Corp Malaysia. They are vital contributors to economic growth and key stakeholders in digital transformation initiatives.
The Fourth Industrial Revolution (4IR)	Describe the current fusion of technologies that is blurring the lines between the physical, digital, and biological spheres. This revolution is characterised by a range of technologies that are reshaping industries and societies:
The National Critical Information Infrastructure	A computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively.
Vendor Lock-In	A situation where a customer becomes dependent on a single cloud service provider, making it difficult to switch to another provider without substantial costs or disruption.

POLICY DIRECTION

The NCCP (National Cloud Computing Policy) is a comprehensive policy that applies to all sectors (government agencies, private businesses, and citizens) within Malaysia's jurisdiction. It provides a strategic roadmap for cloud adoption, driving innovation, economic resilience, and digital inclusivity to achieve the nation's digital transformation goals.

This policy serves as an overarching framework for the entire cloud ecosystem in Malaysia. It provides a clear direction for stakeholders across all sectors to develop their own specific policies or guidelines tailored to their unique requirements and circumstances. This approach ensures flexibility and adaptability within a unified national strategy. This policy is in line with the existing public sector cloud computing policy.

The policy directs stakeholders to:

- *Anticipate: Identify and assess potential challenges and opportunities related to cloud computing across all sectors.*

- *Call to Action: Develop and implement strategies and actions to address identified risks and opportunities.*

This NCCP is designed as a living document, without a fixed duration or timeframe. This is crucial because the cloud computing landscape is constantly evolving with new technologies, services, and challenges emerging regularly. The document allows for continuous updates and revisions, ensuring the policy remains relevant and effective in guiding Malaysia's cloud computing journey. This approach promotes agility and responsiveness, enabling the nation to stay ahead of the curve in the dynamic world of cloud computing.

MADANI CONCEPT

The document incorporates the concept of Madani by emphasising inclusivity, equitable access, and societal well-being within its cloud computing framework. It aims to bridge the digital divide, empower communities, and ensure that cloud technology enhances public services like healthcare and education, benefiting all Malaysians. Furthermore, the policy promotes ethical considerations, data privacy, and security to foster trust and social cohesion, aligning with the principles of sustainable development by advocating for environmentally friendly cloud practice.

filter(
length
src_size
estimate
float
for i

EXECUTIVE SUMMARY -
Malaysia's Cloud Vision at a Glance

What is the National Cloud Computing Policy?

The National Cloud Computing Policy (NCCP) or *Dasar Pengkomputeran Awan Negara*, sets Malaysia's strategic pathway for cloud adoption, driving innovation, economic resilience, and digital inclusivity to achieve the nation's digital transformation goals.

The NCCP aligns with key national digital strategies, including the Malaysia Digital Economy Blueprint (MyDIGITAL), which seeks to position Malaysia as a regional leader in the digital economy; the National Fourth Industrial Revolution (4IR) policy, which emphasises leveraging advanced technologies to propel Malaysia into a technology-driven future; Malaysia Cyber Security Strategy (MCSS), which ensures robust data protection and cybersecurity measures are in place to support cloud adoption; and the New Industrial Master Plan 2030, which adopts a mission-based approach to collectively guide Malaysia's industries toward technological advancement, sustainability, and deeper integration into the global value chain.

Cloud computing provides the scalable infrastructure and computational power necessary to support emerging technologies like artificial intelligence (AI) applications, enabling faster processing, enhanced data storage, and the seamless integration of machine learning models across diverse industries.

In addition, the NCCP supports broader national development strategies like RMK13 (Rancangan Malaysia Ke-13), which prioritises economic resilience, sustainability, inclusive growth, and regional balance. By fostering high-value investments and creating a conducive environment for innovation, the NCCP directly contributes to RMK13's goals of empowering SMEs, enhancing public services through digital transformation, and driving regional competitiveness. Central to the NCCP is fostering a regulatory environment that encourages public-private partnerships and investment opportunities. The policy seeks to create an adaptable cloud ecosystem that empowers government agencies, businesses, and citizens alike - setting the stage for a vibrant, resilient, and sustainable digital Malaysia.

Why do we need a National Cloud Computing Policy?

As Malaysia moves forward with its digital transformation, adopting a robust cloud policy is crucial for unlocking the full potential of cloud technology across all sectors. The NCCP will enhance Malaysia's global competitiveness by ensuring that its digital infrastructure meets high security standards. Without a coordinated cloud strategy, Malaysia risks lagging behind in the rapidly evolving digital economy and may face challenges in achieving its goals for a secure, inclusive, and efficient digital ecosystem.

This policy lays the groundwork for strategic collaboration and investment that can accelerate growth and bolster both local and global partnerships. Cloud adoption also empowers businesses, particularly small and medium enterprises (SMEs), by providing access to innovative and scalable technologies. Additionally, by supporting digital inclusivity, the NCCP ensures that the benefits of cloud technology reach all Malaysians, regardless of geographical or socio-economic barriers.

Goals

The NCCP sets clear aspirations for Malaysia's cloud ecosystem, aiming to:

Establish Malaysia as a leading regional cloud and digital hub by 2030

Enhance public sector efficiency through improved digital service delivery

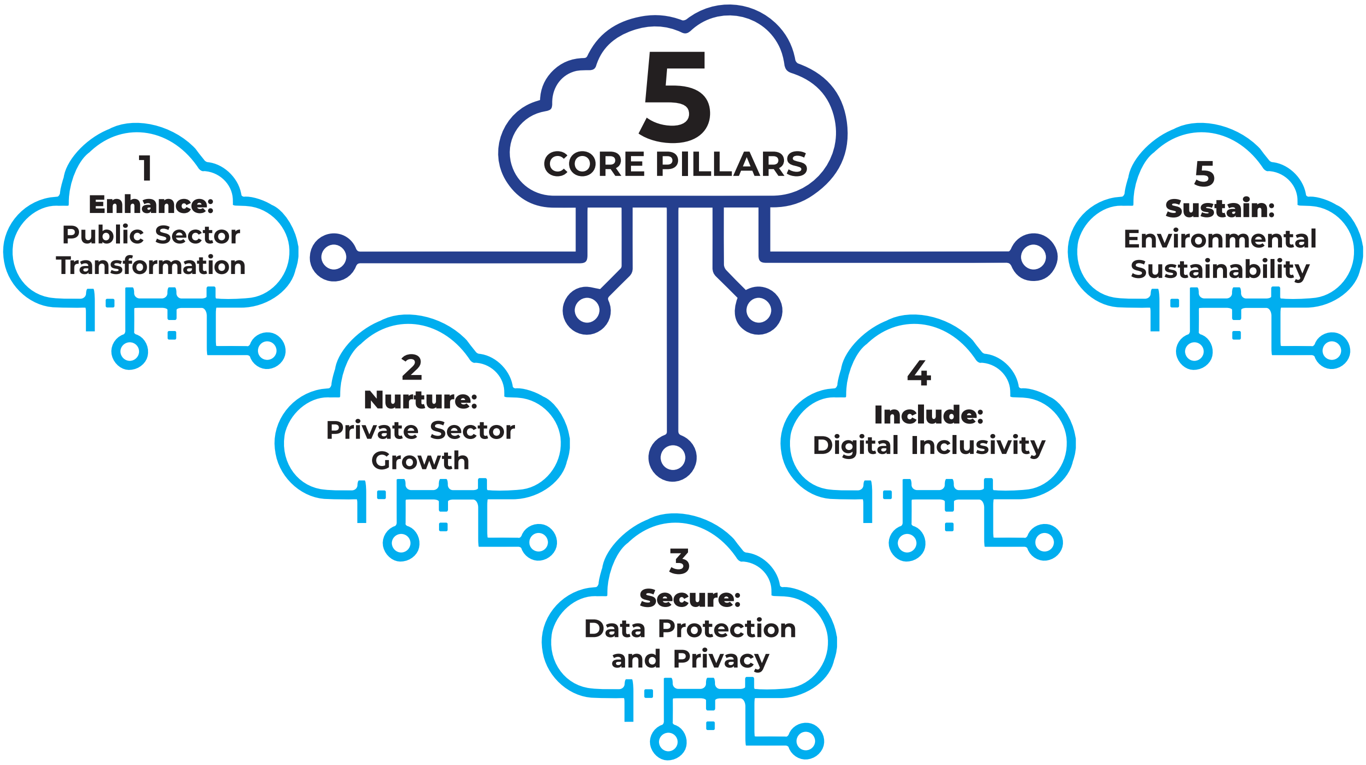
Foster private sector competitiveness and innovation through cloud technology

Enable a digitally inclusive society

Promote resource-efficient and environmentally friendly cloud practices

Strategic Focus of the NCCP

To achieve these goals, the NCCP focuses on five core pillars guiding cloud adoption in Malaysia:



Together, these pillars form a strategic and inclusive foundation for Malaysia's cloud vision, aligning with the nation's broader aspirations for digital transformation.

The NCCP also enables the development of the infrastructure necessary to support emerging technologies, creating a secure and scalable environment that drives innovation across key sectors like healthcare, finance, and education.By promoting investments in cloud computing and data centres, the NCCP reinforces Malaysia's commitment to becoming a leader in technology-driven innovation and economic resilience.

To realise these aspirations, targeted initiatives across each pillar are designed to maximise strategic growth while facilitating coordinated progress across Malaysia's cloud ecosystem.

Whole-of-Nation Approach

The NCCP embraces a Whole-of-Nation approach to foster collaboration across all sectors of Malaysian society. Government agencies, the private sector, and citizens all play a unique and indispensable role in supporting Malaysia's cloud journey. This collective effort supports the development of a secure, inclusive, and future-ready digital nation.

By uniting these stakeholders in a shared vision, Malaysia can fully harness cloud technology to drive sustainable growth, enhance global competitiveness, and ensure that all Malaysians have access to digital opportunities—ultimately empowering them to thrive in the evolving digital economy.

PART 1: STRATEGIC FOUNDATION FOR MALAYSIA'S CLOUD VISION

1.1 Vision and Mission Statement

Vision : *"Position Malaysia as the leading global cloud hub".*

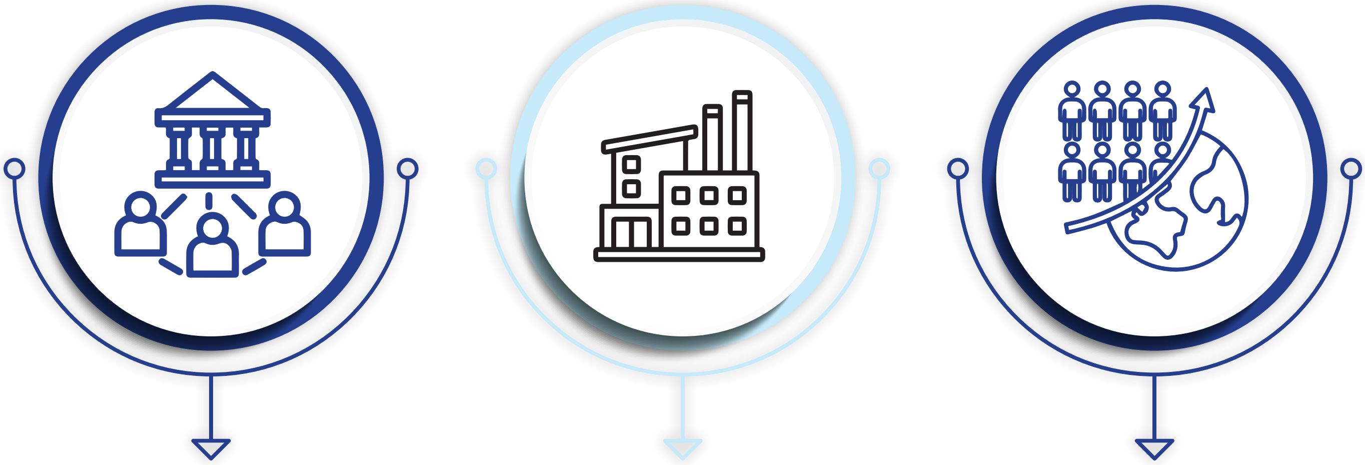
To establish Malaysia as a global frontrunner in cloud technology by 2030, recognised for its innovation, security, and commitment to sustainability. By building a robust cloud ecosystem with world-class infrastructure, skilled talent, and advanced cybersecurity, Malaysia will become the global premier cloud hub, setting global benchmarks in cloud technology while driving economic resilience and societal progress.

Mission : *"Drive Malaysia's digital transformation through cloud adoption".*

Our mission is to drive Malaysia's digital transformation by fostering the adoption of innovative, secure and adaptable cloud technologies. Through a resilient cloud infrastructure, we will enhance the capabilities of both the public and private sectors and create an inclusive digital ecosystem. Through collaboration, nurturing talent, and embracing sustainable practices, we will build a future where every citizen and business can thrive in Malaysia's vibrant, competitive and globally recognised digital economy.

1.2 Policy Statement

The NCCP establishes a framework for a secure, efficient, and sustainable cloud adoption across Malaysia's public, private, and citizen sectors, positioning cloud computing as a cornerstone of the nation's digital transformation. The policy outlines the roles and responsibilities for each sector:



PUBLIC SECTOR

The NCCP serves as a mandate for cloud adoption within government agencies to enhance efficiency and improve citizen services. Agencies must comply with relevant laws, policies and standards, ensuring alignment with cost-efficiency goals and service excellence objectives.

PRIVATE SECTOR

Cloud adoption is encouraged to drive innovation and competitiveness within the private sector. While adoption is generally voluntary, compliance is necessary where legal obligations exist.

CITIZENS

The policy adopts a citizen-centric approach, prioritising data protection, privacy, and equitable access to cloud services. It empowers citizens to utilise cloud services confidently, assured of an accessible, secure and inclusive digital environment.

By addressing each stakeholder's role clearly, the NCCP fosters a secure, inclusive, and innovative cloud ecosystem, accelerating Malaysia's digital transformation.

1.3 Malaysia's Strategic Digital Ambitions

The NCCP is a key enabler of the country's broader digital transformation, aligning with the priorities of **MyDIGITAL**, the **4IR Policy**, and the **New Industrial Master Plan 2030 (NIMP)**. These strategies share a vision of growth, competitiveness, and inclusivity which the NCCP supports through a secure, scalable and sustainable cloud framework.

SUPPORTING MYDIGITAL

The NCCP strengthens MyDIGITAL's focus on economic competitiveness and inclusive digital infrastructure by promoting cloud adoption across various sectors, from government to SMEs. By prioritising a "cloud-first" approach, the NCCP enhances public service delivery, expands digital access for all Malaysians, and supports Malaysia's goal of becoming a regional digital hub through cloud infrastructure investment[1].

ADVANCING THE 4IR POLICY

Cloud computing is one of the core technologies in the 4IR Policy, supporting Malaysia's digital economy through advanced capabilities such as AI, IoT, and Big Data. By establishing a robust and secure cloud ecosystem, the NCCP underpins 4IR advancements and prepares Malaysia for future technology adoption[2].

COMPLEMENTING NIMP 2030

While NIMP 2030 does not specifically mention cloud computing, the NCCP's focus on sustainable cloud practices supports NIMP's vision for fostering technological advancements and increased industrial competitiveness. By promoting climate-resilient and resource-efficient cloud infrastructure, the NCCP aligns with NIMP's goal to strengthen enablers for sustainable growth, contributing indirectly to Malaysia's ambitions for low-carbon, environmentally responsible industrial practices.

MALAYSIA CYBER SECURITY STRATEGY

The Malaysia Cyber Security Strategy (MCSS) is a comprehensive framework aimed at bolstering the country's cybersecurity landscape. It was developed in response to the increasing cyber threats and the need to protect the nation's digital assets.

Through these strategic alignments, the NCCP unifies cloud infrastructure as an essential element to achieving Malaysia's broader national objectives.

[1] MyDIGITAL
Thrust 1: Drive Digital Transformation in the Public Sector
Thrust 2: Boost Economic Competitiveness Boost Economic Competitiveness through Digital Adoption – *"To grow the digital economy by promoting digital adoption among businesses, including SMEs, and strengthening Malaysia's position as a competitive digital economy."*
Thrust 3: Build Enabling Digital Infrastructure – *"Ensure inclusive digital connectivity and access across Malaysia, with a focus on underserved areas, to bridge the digital divide."*

[2] 4IR Policy
Policy Thrust 3: Future-Proof Regulations to Be Agile with Technological Changes – *"To establish secure, future-ready regulations that support technological change while prioritising data sovereignty, security, and ethical standards."*
Policy Thrust 4: Accelerate 4IR Technology Adoption – *"Drive the adoption of Fourth Industrial Revolution technologies across government, business, and society to boost productivity and efficiency."*

1.4 Key Objectives for National Progress

The NCCP is designed around four core objectives that form the foundation of Malaysia's cloud vision:

1. ENHANCING PUBLIC SERVICE EFFICIENCY AND INNOVATION	**Objective** Accelerate the adoption of cloud solutions in government agencies to improve public service delivery, streamline operations, and enhance citizen engagement.	**Impact** Modernise government systems and enable better access to digital services, improving responsiveness and transparency.
2. DRIVING ECONOMIC GROWTH AND COMPETITIVENESS	**Objective** Drive economic growth through global partnerships, enabling businesses, particularly SMEs and startups, in leveraging cloud technologies to foster innovation, increase operational efficiency, and access global markets.	**Impact** Boost economic growth by providing scalable, cost-effective cloud solutions that help businesses innovate and expand.
3. STRENGTHENING DATA SECURITY AND PUBLIC TRUST	**Objective** Implement robust security frameworks to ensure the protection of data in both public and private cloud environments, increasing trust among users.	**Impact** Enhance the credibility of cloud services by ensuring compliance with data protection laws and fostering trust in digital platforms.
4. EMPOWERING CITIZENS THROUGH DIGITAL INCLUSIVITY	**Objective** Deliver accessible public services through a citizen-centric, digital-first approach that leverages cloud technologies for greater inclusivity.	**Impact** Reduce the digital divide, enabling citizens to benefit from seamless, accessible, and secure online services, and promoting a digitally empowered society.

PART 2: WHY CLOUD MATTERS FOR MALAYSIA'S FUTURE

2.1 Strategic Importance of Cloud Computing

Cloud computing is foundational to digital strategies worldwide, driving economic growth, improving efficiency, and fostering inclusivity. According to IDC, global cloud spending is projected to reach $805 billion by 2024 and could double by 2028[3]. In Malaysia, cloud computing plays a crucial role in unlocking potential across sectors, from public administration to SMEs. Without a robust cloud infrastructure, Malaysia risks falling behind in the global digital economy, especially as other countries advance cloud adoption to drive competitive and inclusive growth.

2.2 What is Cloud Computing?

Cloud computing is a strategic technology model that enables on-demand, scalable convenient access to shared pools of configurable resources, such as networks, servers, storage, and applications, with minimal management effort. This technology enhances operational agility and cost efficiency, while fostering innovation, across both public and private sectors.

The National Institute of Standards and Technology (NIST) defines cloud computing through five essential characteristics[4]:

ON-DEMAND SELF-SERVICE

Users can autonomously access computing resources.

BROAD NETWORK ACCESS

Resources are accessible over networks, enhancing mobility and accessibility.

RESOURCE POOLING

Cloud providers dynamically allocate resources to meet user demand.

RAPID ELASTICITY

Resources can scale quickly, adapting to varying workloads.

MEASURED SERVICE

Usage is monitored, promoting efficiency and cost-effectiveness.

These characteristics provide scalable and flexible IT solutions that drive Malaysia's broader digital transformation goals.

[3] IDC Worldwide Software and Public Cloud Services Spending Guide – from article *'Worldwide Spending on Public Cloud Services is Forecast to Double Between 2024 and 2028, According to New IDC Spending Guide'* - https://www.idc.com/getdoc.jsp?containerId=prUS52460024

[4] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

2.3 National and Global Trends

Cloud adoption is growing worldwide as countries recognise its role in driving digital economies. In the Asia-Pacific region, cloud computing contributes up to 2.23% of GDP in certain economies . Public cloud spending in Asia is projected to reach $500 billion by 2025, driven by digital transformation initiatives and rising demand for IT infrastructure[6].

GLOBAL SPENDING

Gartner projects that global public cloud services spending will increase by 20.4% in 2024, reaching $675.4 billion[7]. By 2028, 70% of tech workloads are expected to run in the cloud[8], fuelled by emerging technologies like generative AI and application modernisation.

PUBLIC SECTOR

In Malaysia, the MyGovCloud initiative target has achieved 80% of cloud storage adoption across public sector in 2022 and currently the government is focusing on cloud-native implementation.

MALAYSIA'S LOCAL MARKET OVERVIEW

Malaysia's public cloud market is expected to reach US$1.967 billion by 2024, with a CAGR of 20.52% between 2024 and 2029[10]. The largest segment remains Infrastructure-as-a-Service (IaaS), projected at US$609.8 million by 2024[11]. Investment in Malaysia's cloud infrastructure has been substantial, with over RM114.7 billion approved by 2023[12], and global CSPs , including AWS, Microsoft, Google, and Oracle, are collectively committing more than US$16.5 billion by 2024[13].

In 2023, the Knight Frank SEA-5 Data Centre Opportunity Index ranked Malaysia as the top destination for data centre investment in Southeast Asia, citing high GDP growth, a surge in interest in cloud services, and favourable government initiatives[14]. Malaysia saw a substantial 113 MW data centre take-up in 2022, far surpassing Thailand's 25 MW. Key growth areas include Kuala Lumpur and Johor, benefiting from spillover effects from Singapore.

MALAYSIA'S ECONOMIC IMPACT

Malaysia is projected to have a significant positive economic impact[15].

A 1% increase in cloud adoption in 2023 is estimated to add 10.5 billion Malaysian ringgit (approximately $2.23 billion) to Malaysia's GDP.From 2024 to 2028, Malaysia could unlock up to 110 billion Malaysian ringgit (approximately $23.25 billion) in additional economic value through expanded cloud service usage, contingent on government policies. Organisations migrating to cloud platforms like AWS have seen potential reductions in total cost of ownership (TCO) by up to 66% for compute, networking, and storage, alongside improvements in performance, efficiency, and agility.

Despite this growth, the SME sector—which make up 96.9% of businesses in Malaysia[15]— have been slower in adopting cloud technologies due to perceived high transition costs and concerns over immediate financial returns[16]. As of 2020, only around 44% of SMEs had adopted cloud computing[17].

This regional and global momentum underscores the urgency for Malaysia to strengthen its cloud infrastructure and integrate it across all sectors to remain competitive.

[5] Asian Development Bank. (2024). *Cloud computing policies and their economic impacts in Asia and the Pacific.* https://www.adb.org/publications/cloud-computing-policies-and-their-economic-impacts-in-asia-and-the-pacific
[6] Tech Wire Asia. (2023). *Cloud computing market expected to reach US$500 billion by 2025*. Tech Wire Asia. https://techwireasia.com/2023/05/cloud-computing-market-expected-to-reach-us500-billion-by-2025/
[7] The Edge Markets. (2024). *Global public cloud end-user spending to hit US$675b in 2024, says Gartner.* https://theedgemalaysia.com/node/712402
[8] Gartner. (2023). *Cloud modernisation will see 70% of workloads in cloud environments by 2028*. TechRepublic. https://www.techrepublic.com/article/gartner-cloud-computing-predictions-australia/
[9] Bernama. (2022). *"Govt Introduces Cloud Computing Service MyGovCloud."* www.bernama.com/en/news.php?id=2079174.
[10] Statista. (2024). Public Cloud - Malaysia | Statista Market Forecast. https://www.statista.com/outlook/tmo/public-cloud/malaysia
[11] Statista. (2024). Software as a Service - Malaysia | Statista Market Forecast. https://www.statista.com/outlook/tmo/public-cloud/software-as-a-service/malaysia
[12] Malaysian Investment Development Authority (MIDA). (2024). *Malaysia approved RM114.7 billion investments in data centres and cloud services from 2021 to 2023."* https://www.mida.gov.my/mida-news/malaysia-approved-rm114-7-bln-investments-in-data-centres-cloud-services-from-2021-to-2023/
[13] The Star. (2024, November 4). Tech giants to continue investing in data centres. https://www.thestar.com.my/business/business-news/2024/11/05/tech-giants-to-continue-investing-in-data-centres
[14] Malaysia Digital Investment Office (2024). *Data Centre & Cloud*. https://mydigitalinvestment.gov.my/data-centre-cloud
[15] *AWS Economic Development (2024), "AWS Economic Impact Study", Amazon Web Services, Inc., https://asean-resources.awscloud.com/aws-in-malaysia/malaysia-economic-impact-study*
[16] SME Corp Malaysia. (2023). *Profile of MSMEs in 2015-2023*. https://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/profile-and-importance-to-the-economy
[17] Twimbit Insights (2023). "Public Cloud Spending in Malaysia." https://twimbit.com/insights/public-cloud-spending-in-malaysia
[18] Tong, A., & Gong, R. (2020). Digitalisation of firms: Challenges in the digital economy. Khazanah Research Institute. https://www.krinstitute.org/assets/contentMS/img/template/editor/20201005%20Digitalisation%20Challenges%20v3.pdf

2.4 Enablers and Barriers to Cloud Adoption

Effective cloud adoption depends on addressing key enablers while overcoming significant barriers.

BENEFITS

EFFICIENCY AND VALUE FOR MONEY
Cloud technology minimises the need for costly physical infrastructure, enabling organisations to manage resources more effectively with pay-as-you-use models.

SCALABILITY AND AGILITY
Cloud platforms allow organisations to quickly scale operations and adapt to market demands, fostering innovation.

ENHANCED COLLABORATION AND ACCESS
Improved data sharing and collaboration capabilities across departments and sectors facilitate seamless workflows.

ENVIRONMENTAL IMPACT
Shared cloud infrastructure and energy-efficient data centres contribute to reducing carbon footprints.

ENABLERS

GOVERNMENT INITIATIVES
Programs like MyGovCloud and MyDIGITAL's "cloud-first" policy are essential for driving cloud adoption, particularly in the public sector. SASARAN FASA KEDUA MYDIGITAL - INISIATIF :N2S3I1 (EMERGING TECHNOLOGY, OPEN API: CLOUD-FIRST)

STRATEGIC PARTNERSHIPS WITH CLOUD SERVICE PROVIDERS (CSPs)
Collaborations with leading CSPs will strengthen Malaysia's cloud infrastructure and regional positioning.

PUBLIC-PRIVATE COLLABORATION
Partnerships between government and private entities help standardise cloud practices, aligning with global standards and ensuring resilience.

DIGITAL LITERACY AND WORKFORCE DEVELOPMENT
Initiatives to boost digital literacy and cloud-specific skills address workforce gaps, building a cloud-competent talent pool.

INCENTIVES FOR SMES
Financial support, including grants and tax relief, assists SMEs in overcoming cost-related barriers, enhancing competitiveness.

TECHNOLOGY HUBS AND INNOVATION CENTRES
Establishing innovation hubs supports research in cloud computing, AI, and related fields, positioning Malaysia as a leader in the digital economy.

BARRIERS

DATA SECURITY, PRIVACY, AND SOVEREIGNTY CONCERNS

Elevated risks in cloud environments necessitate strict policy and controls to address unauthorised access, data privacy, and sovereignty issues, especially for data stored cross-border.

REGULATORY FRAGMENTATION

Inconsistent policies across sectors create compliance challenges for CSPs and businesses, leading to confusion and slowing cloud adoption. Streamlined regulations are needed to foster a predictable, business-friendly environment.

ECONOMIC BARRIERS

High initial costs for cloud migration and ongoing expenses pose significant challenges, particularly for SMEs and underserved regions.

INFRASTRUCTURE LIMITATIONS

Current public sector systems and limited infrastructure in rural areas hinder seamless cloud integration.

SKILL GAPS

A shortage of skilled cloud professionals restricts effective cloud adoption. Workforce development programs are essential for cultivating local expertise.

PUBLIC TRUST AND AWARENESS

Limited understanding and awareness of cloud benefits contribute to public scepticism, affecting adoption rates.

INTEROPERABILITY ISSUES

Challenges in integrating cloud solutions with legacy systems lead to higher migration costs and reduced operational

VENDOR LOCK-IN RISKS

Heavy reliance on specific CSPs can restrict adaptability and incur high switching costs, posing long-term challenges for organisations.

2.5 Cloud Computing Models and Deployment Options

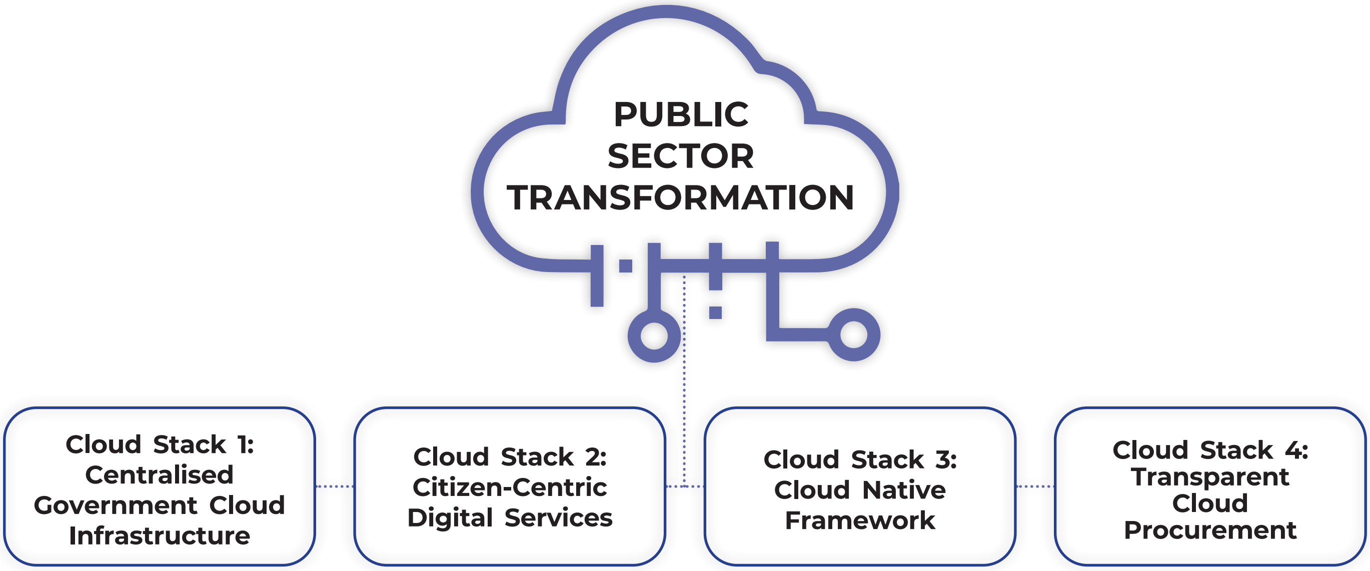
The NCCP recognises a variety of cloud models and service types to address Malaysia's diverse needs across sectors. Details on deployment models, such as public, private, hybrid, community, and multi-cloud, and service types, such as IaaS, PaaS, SaaS, are provided in **Appendix A.** These models and services cater to Malaysia's diverse needs, addressing requirements for security, data sovereignty, and operational flexibility.

PART 3: CORE PILLARS DRIVING MALAYSIA'S CLOUD VISION

Introduction

The NCCP is built around five core **Pillars**, each focused on a specific aspect of Malaysia's national digital strategy. Each Pillar is broken down into **Cloud Stacks**, which define the objectives and specific actions needed to build a secure, scalable, and resilient cloud ecosystem for the nation.

PILLAR 1 – ENHANCE



PUBLIC SECTOR TRANSFORMATION

Cloud Stack 1: Centralised Government Cloud Infrastructure

Cloud Stack 2: Citizen-Centric Digital Services

Cloud Stack 3: Cloud Native Framework

Cloud Stack 4: Transparent Cloud Procurement

Cloud Stack		Policy Direction
CS 1 Centralised Government Cloud Infrastructure	Develop unified cloud infrastructure and platform for government operations.	Establish a robust, secure, and scalable centralised cloud infrastructure that serves as the foundation for all public sector digital services, ensuring cost-efficiency, resilience, and sustainability.
CS 2 Citizen-Centric Digital Services	Enhance citizen engagement, service delivery and accessibility through digital government services.	Provide accessible, secure, and user-centric digital services for all citizens. Leverage cloud infrastructure to better meet citizens' needs, with a focus on inclusivity for underserved populations and safeguarding personal data.
CS 3 Cloud Native Framework	Promote cloud-based applications for government optimised for cloud from inception.	Foster the adoption of cloud-native technologies across public sector to promote innovation, scalability, and operational efficiency. Leverage modern architectures such as microservices, containers, and serverless computing to enable agile and resilient services that adapt to evolving citizen demands.
CS 4 Transparent Cloud Procurement	Ensuring fair & transparent practices in government cloud procurement.	The implementation of cloud procurement will be subject to the approval of the Ministry of Finance (MOF), with enhancements made to streamline the process to meet the needs of cloud deployment across the public sector. This will involve adopting an open tender process to ensure transparency, fairness, and competitiveness. Procurement processes will be aligned with clear guidelines to award contracts based on performance metrics, cost-effectiveness, and alignment with national priorities. Additionally, well-defined Service Level Agreements (SLAs) will be incorporated to ensure accountability in service delivery, fostering trust and delivering measurable outcomes for the government and its stakeholders.

EXAMPLES FOR CLOUD TECHNOLOGY ACROSS INDUSTRIES FOR PILLAR 1 : ENHANCE

Example 1

Saving Lives During Floods : Real-Time Disaster Response -

In recent monsoon seasons, floods have caused widespread damage. Government agencies struggled to coordinate relief efficiently due to fragmented data and communication.

Cloud-Based Data Integration for Disaster Response :

By leveraging a cloud-based data integration platform, government agencies can now access real-time data from various sources—weather updates, flood sensors, emergency services, and citizen reports. The platform makes it easier to share data across agencies, enabling efficient resource allocation, targeted evacuation notices, and quick response for affected communities.

Example 2

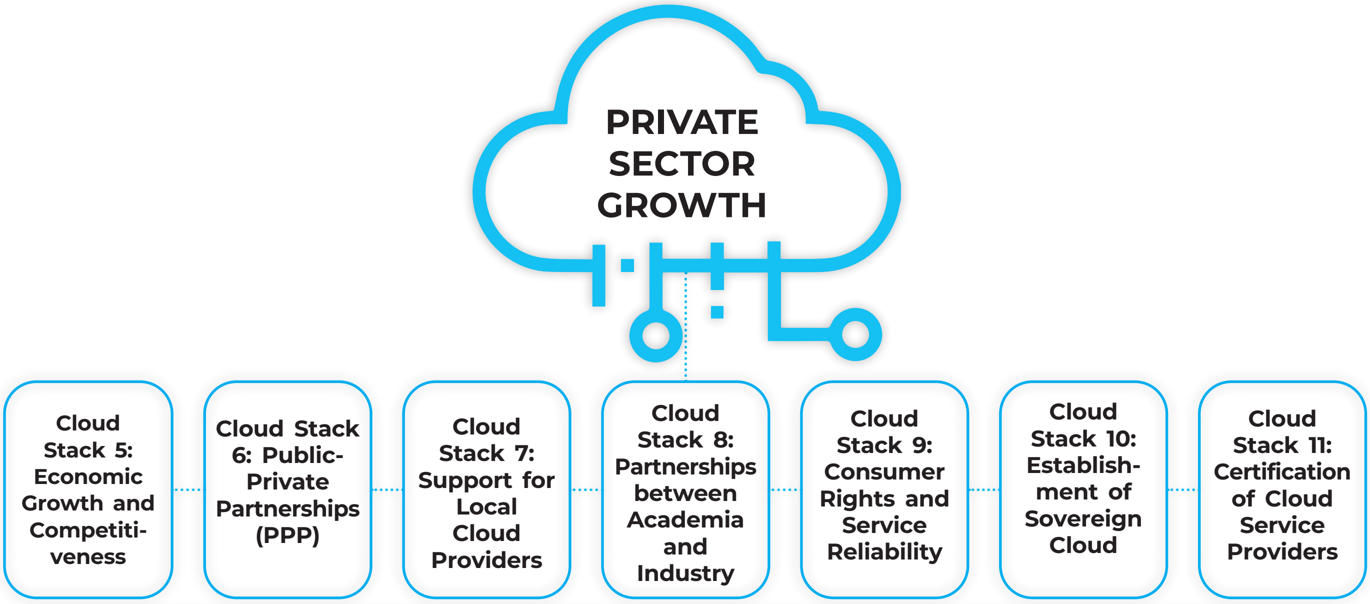
Smoother Journeys : Reducing Traffic Congestion in Kuala Lumpur -

Kuala Lumpur has faced increasing traffic congestion, resulting in delays and pollution. City officials struggled to monitor and manage traffic flow in real-time.

Cloud-Based Traffic Management :

A cloud-enabled traffic management system was implemented, bringing together data from cameras, sensors, and connected vehicles. City authorities now receive real-time analytics and predictive insights to adjust traffic signals, manage incidents, and optimise traffic flow dynamically. The cloud's scalability supports quick and vast data processing, making urban traffic management more efficient and reducing overall congestion, making travel smoother for everyone.

PILLAR 2 – NURTURE



PRIVATE SECTOR GROWTH

Cloud Stack 5: Economic Growth and Competitiveness

Cloud Stack 6: Public-Private Partnerships (PPP)

Cloud Stack 7: Support for Local Cloud Providers

Cloud Stack 8: Partnerships between Academia and Industry

Cloud Stack 9: Consumer Rights and Service Reliability

Cloud Stack 10: Establishment of Sovereign Cloud

Cloud Stack 11: Certification of Cloud Service Providers

Cloud Stack		Policy Direction
CS 5 Economic Growth and Competitiveness	Drive cloud adoption to foster growth, attract investment and enhance innovation.	Drive economic growth, attract foreign investments, and position the country as a competitive digital hub regionally and globally. Foster a vibrant cloud ecosystem that enhances productivity, innovation, and industry competitiveness.
CS 6 Public-Private Partnerships (PPP)	Fostering collaboration between government and private sector in cloud intiatives.	Promote collaboration between public institutions and private CSPs to develop scalable, secure, and cost-effective cloud solutions. Align partnerships with national digital goals to ensure seamless integration of cloud services across all sectors.
CS 7 Support for Local Cloud Providers	Encourage the development and growth of the local cloud industry.	Support for local cloud providers necessitates fostering collaborations that enable infrastructure sharing and improved resource efficiency through the development of cloud marketplaces and incentives for joint ventures. Concurrently, empowering local System Integrators (SIs) and software houses via skills development and encouraged collaboration with CSPs, alongside government support is crucial for strengthening the ecosystem and driving economic growth by creating jobs and specialised solutions.
CS 8 Partnerships between Academia and Industry	Establishing collaborations with academia to develop skilled workforce.	Promote partnerships between academia and industry to drive research and development in emerging cloud technologies. Foster innovation and digital skills development to cultivate a future-ready workforce. Advance cloud technology leadership through knowledge-sharing initiatives and innovation hubs.
CS 9 Consumer Rights and Service Reliability	Promote accountability and trust in cloud services through consumer protection standards.	Ensure accountability and trust in cloud services by establishing robust consumer protection standards. Require CSPs to implement clear Service Level Agreements (SLAs) that define performance metrics and include mechanisms for consumer redress, such as dispute resolution processes, compensation for service failures, and transparent communication channels to address consumer grievances.
CS 10 Establishment of Sovereign Cloud	Establish sovereign cloud infrastructure to comply with data sovereignty standards.	Collaborate with reputable CSPs to establish sovereign cloud infrastructure that adheres to Malaysia's data sovereignty standards. This ensures that critical data is stored, processed, and accessed within national boundaries, aligning with local laws and national security priorities. The sovereign cloud will build trust and enhance regulatory compliance.
CS 11 Certification of Cloud Service Providers	Certify CSPs to ensure compliance and foster a trusted cloud ecosystem.	Establish a multi-tier certification framework for cloud services offered by CSPs, tailored to data sensitivity and security requirements. This framework will ensure CSPs meet established standards and adhere to security benchmarks, fostering trust, transparency, and adoption across sectors.

EXAMPLES FOR CLOUD TECHNOLOGY ACROSS INDUSTRIES FOR PILLAR 2 : NURTURE

Example 1

Scaling Up a Small Business : Ravi's Chilli Sauce Goes Global -

Ravi owns a small chilli sauce business in Penang. He struggled to scale because his team had limited access to larger supply chain systems and insights.

Cloud-based Inventory Management :

With cloud-based solutions, Ravi was able to access a scalable inventory system that integrated with regional suppliers. This helped him manage stock in real-time, collaborate with logistics providers, and scale his production seamlessly, opening up new markets across Southeast Asia.

Example 2

Staying in Business Through Tough Times : Mei Lin's Boutique Goes Digital -

Mei Lin runs a boutique clothing store in Kuala Lumpur. During unexpected disruptions, such as the recent pandemic, her business operations were halted, leading to financial losses.

Cloud-based Business Continuity :

With a cloud-based POS and inventory system, Mei Lin's store could continue selling online even when the physical shop was closed. The cloud ensured secure data backup and real-time updates on sales and inventory, keeping her business going during tough times.

Example 3

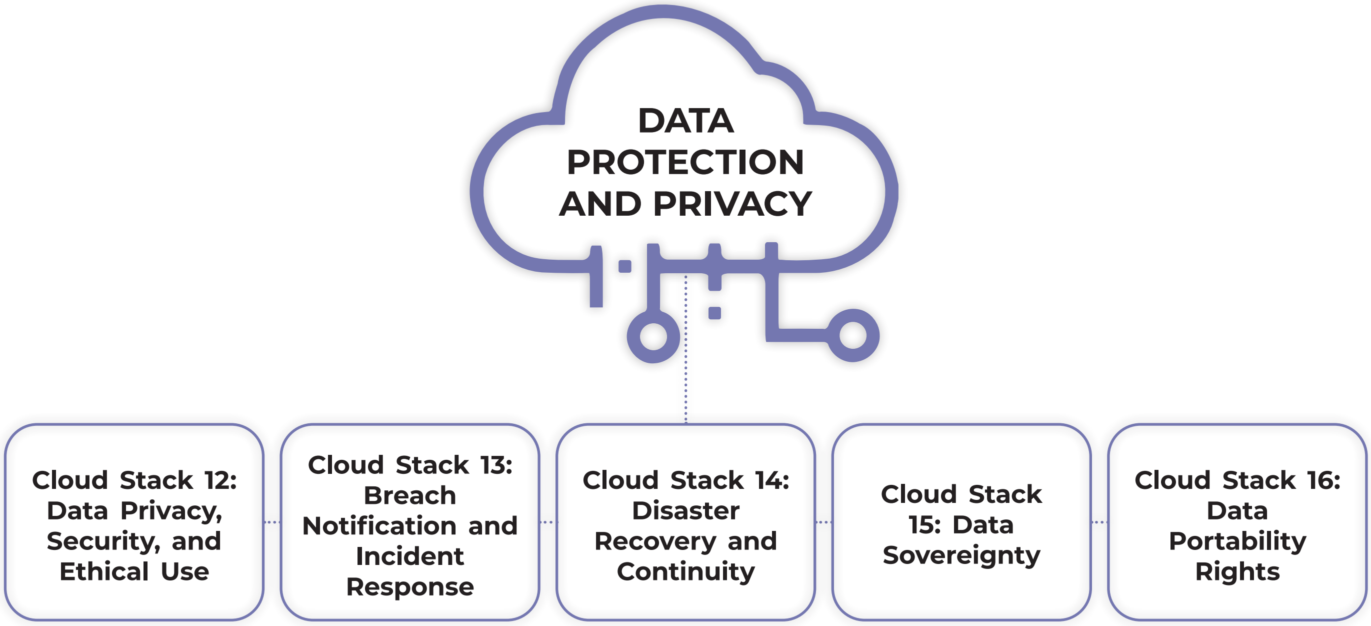
Helping Small Farmers Thrive : Agricultural Advice at Your Fingertips -

Lim, a paddy farmer in Kedah, had limited knowledge about soil health and best farming practices, leading to inconsistent yields.

Cloud-based Advisory Services :

Through a cloud-backed agricultural app, Lim accessed expert advice, soil health data, and crop management practices tailored to his farm. The cloud stored and processed large datasets on soil and climate conditions, enabling personalised recommendations that improved his yield significantly. Lim also gathered other small farmers in his area, sharing the data and insights he received, resulting in collective benefits for the entire community.

PILLAR 3 – SECURE



DATA PROTECTION AND PRIVACY

Cloud Stack 12: Data Privacy, Security, and Ethical Use

Cloud Stack 13: Breach Notification and Incident Response

Cloud Stack 14: Disaster Recovery and Continuity

Cloud Stack 15: Data Sovereignty

Cloud Stack 16: Data Portability Rights

Cloud Stack		Policy Direction
CS 12 **Data Privacy, Security, and Ethical Use**	Protecting data through secure access, privacy controls and ethical standards.	Ensure the highest standards of data privacy, security, and ethical use in cloud services. Adopt stringent data privacy controls and a Zero Trust strategy to protect the integrity, confidentiality, and availability of sensitive information. Safeguard cloud environments against internal and external threats.
CS 13 **Breach Notification and Incident Response**	Ensuring timely breach notifications for transparency and rapid response.	Ensure transparency in breach notifications and establish incident response protocols for cloud-related incidents. Require prompt notification to regulatory bodies to maintain public trust. Ensure thorough response measures to minimise damage and restore normalcy quickly.
CS 14 **Disaster Recovery and Continuity**	Maintaining resilience with disaster recovery and continuity standards.	Establish stringent disaster recovery and continuity protocols for cloud infrastructure to ensure operational continuity of critical services during disruptions, safeguarding public trust and ensuring business continuity.
CS 15 **Data Sovereignty**	Uphold data sovereignty with localisation and jurisdictional compliance.	Uphold data sovereignty by requiring CSPs to comply with national requirements for handling sensitive information. Ensure critical data remains within Malaysia's borders while allowing cross-border data transfers under strict conditions, including encryption, controlled access, and adherence to established standards.
CS 16 **Data Portability Rights**	Empower users with data portability and seamless data transfers.	Empower users by ensuring their right to data portability. Require CSPs to enable seamless transfer of user data between services while maintaining stringent security and privacy standards.

EXAMPLES FOR CLOUD TECHNOLOGY ACROSS INDUSTRIES FOR PILLAR 3 : SECURE

Example 1

Better Healthcare for Rural Communities : Instant Patient Data Sharing -

Dr. Nirmala, working in a community clinic in Sabah, often faced challenges sharing patient records with hospitals in urban centres. This caused delays when patients needed specialised care.

Cloud-based Health Records :

By moving patient records to a cloud-based Electronic Health Record (EHR) system, Dr. Nirmala's clinic could share data securely with hospitals in cities. This allowed specialists to access patients' histories instantly, recommend treatments, and coordinate care efficiently. Cloud computing enabled secure, fast access to critical patient information.

Example 2

Personalised Health Recommendations with AI : Urban Chronic Care Support -

Dr. Rahman, a general practitioner in an urban Selangor clinic, struggled with managing chronic disease patients effectively due to limited decision support.

Cloud-based AI Recommendations :

Using a cloud-based healthcare platform integrated with AI capabilities, Dr. Rahman received recommendations for personalised treatment plans. The system analysed patient histories and current health data to suggest tailored health suggestions for his patients. Throughout this process, patient data was encrypted and securely handled to ensure privacy and compliance with healthcare standards. This enhanced security allowed Dr. Rahman to focus on patient interactions, improving overall care while maintaining trust in data handling practices.

Example 3

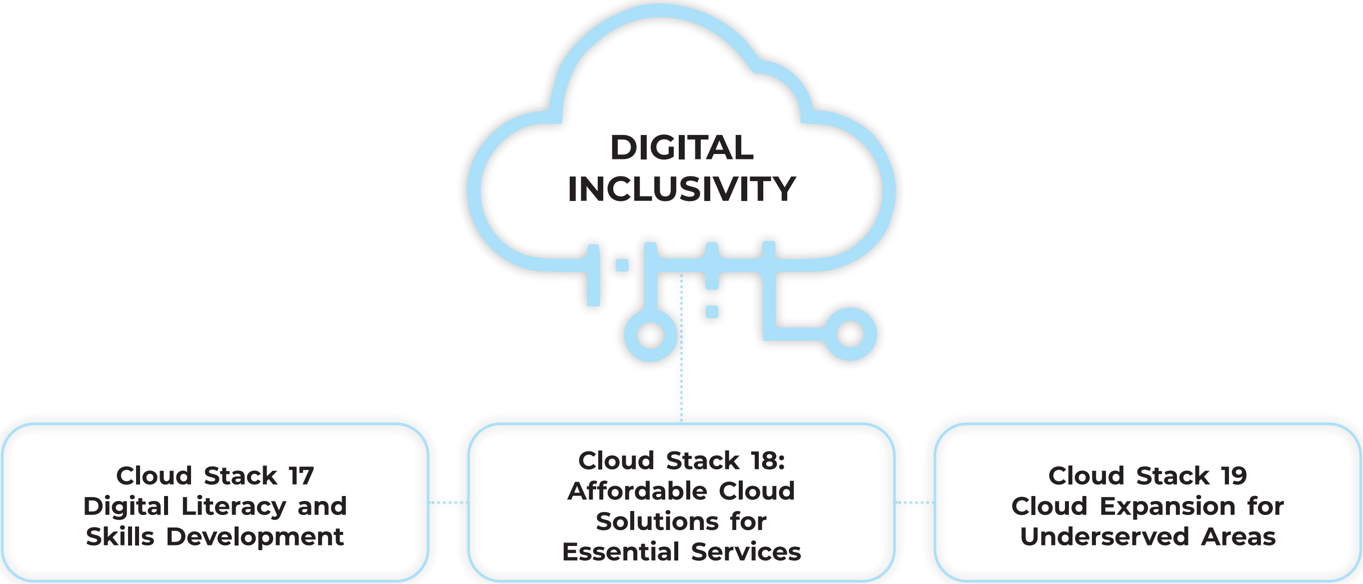
Securing Client Trust with Cloud : A Safer Future for Legal Data -

Rina, a partner at a large law firm, needed to securely manage sensitive client information—financial data, personal records, and case files. Storing this data on local servers made her worried about potential data breaches.

Cloud-based Security and Legal Applications :

By adopting a cloud-based platform, Rina could securely store client data with strong encryption, reducing her concerns about data breaches. Cloud computing ensured high security compliance, keeping sensitive information safe and giving her the confidence needed to protect her clients' data effectively. Additionally, Rina now has access to cloud-based legal apps, such as document management tools, research databases, and AI-powered case assessment tools, which make her work easier and more efficient.

PILLAR 4 – INCLUDE



DIGITAL INCLUSIVITY

Cloud Stack 17 Digital Literacy and Skills Development

Cloud Stack 18: Affordable Cloud Solutions for Essential Services

Cloud Stack 19 Cloud Expansion for Underserved Areas

Cloud Stack		Policy Direction
CS 17 Digital Literacy and Skills Development	Invest in cloud skills training and educations.	Promote digital literacy and skills development across all communities, with a focus on rural areas and marginalised sectors of society. Implement community-based digital empowerment programs and cloud awareness initiatives in collaboration with the private sector and academic institutions to equip citizens with the essential skills needed to thrive in the digital economy.
CS 18 Affordable Cloud Solutions for Essential Services	Promote affordable cloud solutions for sectors like healthcare and education.	Leverage affordable cloud solutions to enhance access and efficiency of essential public services such as healthcare and education.
CS 19: Cloud Expansion for Underserved Areas	Expand cloud infrastructure and connectivity to underserved regions.	Close the digital divide by expanding cloud infrastructure to underserved areas, focusing on rural and remote regions. Promote equitable access to affordable cloud services through targeted investments and policies that encourage private sector participation, empowering underserved communities to engage in the digital economy.

EXAMPLES FOR CLOUD TECHNOLOGY ACROSS INDUSTRIES FOR PILLAR 4 : INCLUDE

Example 1

Bringing Quality Education to Rural Sarawak : Up-to-Date Learning Resources -

Teacher Anita, in a rural Sarawak village, faced challenges accessing quality educational content. She often relied on outdated materials, limiting the learning experience for her students.

Cloud-based Learning Platform :

Using a cloud-powered learning platform, Anita could access the latest educational resources and interact with other educators. The platform offered scalable content access, real-time updates, and interactive tools that improved students' learning. Using cloud services, Teacher Anita can access the latest educational resources, even in remote areas. This helps her students learn better with up-to-date materials, even when internet access is unreliable.

Example 2

Reviving Tourism : Attracting Divers with Smart Cloud Tools -

Nurul operates a dive centre on a remote island in Sabah, but struggles with marketing and managing bookings, particularly during off-peak seasons.

Cloud-based Tourism Platform :

Using a cloud-based booking and tourism platform, Nurul could efficiently manage her dive centre operations, target niche tourists via data-driven marketing, and provide real-time availability updates. Cloud integration with international booking sites increased visibility, helping Nurul attract more visitors during off-peak seasons.

Example 3

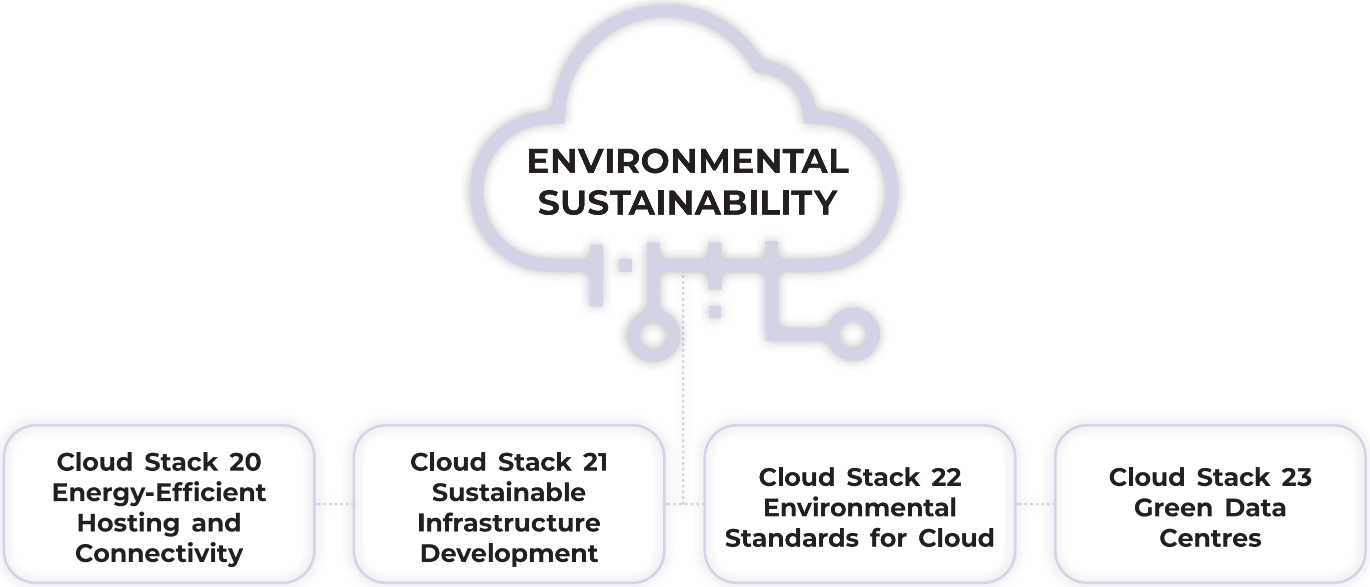
Safe at Sea : Empowering Fishermen with Weather and Price Insights -

Idris and his peers, coastal fishermen in Terengganu, did not have data on weather patterns and market prices, limiting their earnings and increasing risks.

Cloud Analytics :

With a cloud-based mobile app, they received real-time analytics on weather, tides, and fish prices. The app's backend relied on cloud computing to gather and process vast data sets, delivering insights that helped Idris and other fishermen decide the best times to go out to sea, and where to sell for maximum profit.

PILLAR 5 – SUSTAIN



ENVIRONMENTAL SUSTAINABILITY

Cloud Stack 20 Energy-Efficient Hosting and Connectivity

Cloud Stack 21 Sustainable Infrastructure Development

Cloud Stack 22 Environmental Standards for Cloud

Cloud Stack 23 Green Data Centres

Cloud Stack		Policy Direction
CS 20 Energy-Efficient Hosting and Connectivity	Implement cloud hosting practices that minimise energy consumption and reduce carbon footprint.	Promote energy-efficient hosting and connectivity practices by adopting solutions such as virtualisation, resource pooling, and scalable technologies. Reduce energy consumption, maximise resource utilisation, and contribute to a sustainable digital ecosystem.
CS 21 Sustainable Infrastructure Development	Develop sustainable infrastructure for cloud services to reduce resource consumption and waste.	Develop sustainable cloud and energy infrastructure that supports both environmental goals and economic growth without affecting current and future domestic power demand. Encourage investments in green technologies and foster partnerships to reduce the environmental impact of cloud infrastructure and achieve carbon-neutral goals for cloud infrastructure.
CS 22 Environmental Standards for Cloud Operations	Establish environmental standards and guidelines to promote green and sustainable operations.	Set comprehensive environmental standards for cloud operations, including guidelines for hardware recycling, reducing electronic waste, and lowering carbon footprints.
CS 23 Green Data Centres	Develop green data centres that use renewable energy sources and have reduced carbon emissions.	Promote green data centres powered by renewable energy. Encourage green building practices that minimise water usage and reduce environmental impact during construction to create a sustainable digital economy.

EXAMPLES FOR CLOUD TECHNOLOGY ACROSS INDUSTRIES FOR PILLAR 5 : SUSTAIN

Example 1

Greener Construction Sites : Cutting Energy Use with Cloud Data -

Amir, a project manager for a construction company in Johor, wanted to reduce his projects' environmental impact but lacked insights into energy use across different sites.

Cloud-powered Monitoring :

Using cloud computing, Amir implemented energy usage monitoring across construction sites. Cloud services aggregated data from IoT sensors, giving Amir insights to optimise equipment usage, reduce fuel consumption, and adopt more sustainable practices. By monitoring energy usage at construction sites, Amir can reduce fuel consumption and meet environmental goals, making the sites more sustainable.

Example 2

Smart Energy Management : Optimising Solar Power with Cloud and AI -

Andrew, the owner of a solar farm in Negeri Sembilan, faced challenges in managing power generation and distribution efficiently, especially during peak and off-peak hours. He needed a smarter way to monitor and adjust energy production to minimise waste and ensure a steady power supply.

Cloud and AI Integration for Smart Grid Management :

By using a cloud-based energy management system integrated with AI, Andrew could monitor energy production, predict load requirements, and optimise energy storage in real-time. This cloud solution allowed him to make smarter decisions about energy distribution, reduce waste, and ensure a reliable power supply, making the solar farm more sustainable and efficient. This combination of cloud computing and AI improved the efficiency of energy distribution, reduced waste, and ensured a consistent power supply, contributing to more sustainable energy practices.

PART 4: GOVERNANCE AND OVERSIGHT

This section outlines the governance structure and regulatory framework supporting the NCCP, providing an integrated view of regulatory mechanisms, roles and responsibilities to ensure the effective operation of Malaysia's cloud ecosystem.

4.1 Regulatory Framework Overview

The regulatory framework for the NCCP is built on 2 key principles: ensuring compliance with data protection laws and asserting data sovereignty over data generated within Malaysia.

DATA PROTECTION COMPLIANCE

Data protection compliance ensures that all stakeholders—government agencies, businesses (including SMEs) and citizens—adhere to robust security and privacy standards.

- **National Laws** - Personal Data Protection Act 2010 *[Act 709]*; (PDPA) is the law that governs the processing of personal data in Malaysia, particularly for commercial transactions.
- **International Law and Guidelines** - For entities handling foreign citizens' data or operating internationally, compliance with relevant standards, such as the European Union's General Data Protection Regulation (GDPR), ensures that Malaysian cloud services align with global data protection principles and best practices[18].
- **General Data Protection Measures** - CSPs and other entities are required to implement robust data security protocols aligned with the Data Classification Framework such as-
  - **Encryption** - Secure data during storage (at-rest), transmission (in-motion) and in use.
  - **Access Control** - Implement role-based or attribute-based access control for sensitive/classified information.
  - **Regular Audits** - Conduct periodic audits to ensure compliance with both national laws and international standards.

DATA SOVEREIGNTY PRINCIPLES

Data sovereignty ensures that Malaysian laws govern data generated within the country, with additional measures for specific categories of information.

- **Data Sovereignty** - All data generated in Malaysia remains subject to Malaysian laws, regardless of where it is physically stored or processed.
- **Data Residency Only for Specific Categories** - While most data does not have a general residency requirement, certain types of data are legally required to remain physically within Malaysia's borders due to national security, regulatory or sector-specific obligations.
- **Technological Safeguards for Non-Resident Data** - For data that is not subject to residency requirements but still needs to comply with Malaysian laws, technological safeguards can be employed to maintain sovereignty over such data when it is stored or processed abroad. These safeguards should align with the data classification framework:
  - **Encryption with Sovereign Keys** - Data stored abroad is encrypted using sovereign encryption keys controlled by Malaysian entities, ensuring only authorised personnel in Malaysia can decrypt and access it.
  - **Access Controls and Monitoring** - Strict access controls ensure only authorised users in Malaysia can access sensitive information, even when processed or stored abroad.
  - **Data Masking and Tokenisation** - Sensitive information remains securely within Malaysia, while only anonymised tokens or masked versions are processed globally for analytics or non-critical functions.
  - **Hybrid Cloud Solutions** - A hybrid cloud strategy ensures that critical or sensitive information remains within Malaysia using sovereign clouds, while less sensitive operations leverage global cloud infrastructure for scalability and efficiency.

[20] For Cyber Security Act 2024, NACSA is the lead agency for security and sovereignty governance

[19] The GDPR, while not legally binding in Malaysia, provides a robust framework for data privacy, including provisions for data subject rights and cross-border data transfer safeguards

DATA CLASSIFICATION FRAMEWORK

- To ensure data is handled appropriately based on its sensitivity and risk, the NCCP recommends a classification system to guide entities in categorising their data. Entities are responsible for classifying their data and implementing the necessary safeguards to protect it accordingly.

CLASSIFICATION	CLOUD CONSIDERATIONS	RECOMMENDED SECURITY MEASURES*	EXAMPLES
TIER 1: Public Data	Stored in public clouds	• Regular vulnerability scans and security updates for public-facing infrastructure • Implement DDoS protection measures	Government press releases, public reports
TIER 2: Internal Data	• Public clouds (with restricted access) • Private/hybrid clouds	• Role-based access controls (RBAC) • Encryption during transmission • Data loss prevention (DLP) measures • Regular security awareness training for internal personnel/ organisation	Internal policies, non-sensitive reports
TIER 3: Restricted Data	• Private or sovereign clouds with encryption • Hybrid clouds for non-critical operations	• Strong encryption during storage and transmission • Role-based access controls for personally identifiable information • Multi-factor authentication for sensitive business data • Regular audits for PDPA compliance • Data masking where applicable	• Personal Data: Contact details, healthcare records • Business Data: Trade secrets, patents, operational metadata • Implement data access logging/ monitoring) Regular penetration testing and vulnerability assessments
TIER 4: Confidential Data	Stored only in sovereign cloud zones within Malaysia	• Highest-level encryption with sovereign keys • Strict access controls based on clearance levels • Continuous monitoring with real-time threat detection and automated incident response • Appropriate physical access security to data centres (e.g biometrics) Regular security audits and compliance checks	• Classified government documents • Data related to National Critical Information Infrastructure (NCII)

*The recommended security measures listed are non-exhaustive and may be enhanced on future technological expansion or advancement

	• **Compliance with Sector-Specific Requirements** - While the framework above provides general classifications, all entities must also comply with any sector-specific requirements or guidelines relevant to their operations. Entities should stay informed about updates or new regulations issued by relevant authorities to ensure ongoing compliance as the regulatory landscape evolves. • **Public Sector-Specific Requirements** - Public sector entities must comply with classification requirements under (Official Secrets Act 1972 *[Act 88]*;, which governs the handling of government documents and information according to national cyber security law. These classifications take precedence over the general classification tiers above. Additionally, public sector entities must comply with specific cloud computing guidelines issued by authorities such as *Jabatan Digital Negara* and the Chief Government Security Office. Public sector entities must comply with the data sharing requirements set out in Data Sharing Act 2025 *[Act 864]*.

4.2 Relevant Laws and Standards

The NCCP operates within Malaysia's legal and regulatory framework, ensuring compliance in data protection, cybersecurity, and cloud governance. Key laws include the Cyber Security Act 2024 *[Act 854]*; which safeguards National Critical Information Infrastructure; (Communications and Multimedia Act 1998 *[Act 588]*); governing CSP licensing; the (Personal Data Protection Act 2010 *[Act 709]*); , which is central to data protection compliance; and Data Sharing Act 2025 *[Act 864]* which governs the data sharing requirements among government entities.

For more details, please see **Appendix B: Relevant Laws and Standards.**

4.3 Designated Roles and Responsibilities

Clear roles and responsibilities are essential for the effective implementation of the NCCP. Stakeholders across the public sector, private sector, and citizens, must work in tandem to ensure accountability and coordination across the cloud ecosystem.

Public Sector	
CLOUD-FIRST APPROACH IN PROCUREMENT	Public sector agencies must adopt a "cloud-first" approach, prioritising cloud computing solutions in new and existing service procurements. This ensures that cloud solutions are central to infrastructure planning and procurement decisions.
DATA SECURITY AND PRIVACY	Agencies must ensure compliance with national laws and adopt secure practices for managing classified data in accordance with the Official Secrets Act 1972. Due diligence and risk assessment must be conducted.
INTEROPERABILITY AND OPEN STANDARDS	Cloud solutions for the public sector must support interoperability and be based on open standards to reduce vendor lock-in and facilitate seamless data exchange.
GUIDELINES AND PROCUREMENT SUPPORT	Effective cloud adoption requires supportive guidelines and procurement processes. Existing instruments, such as frameworks and procurement policies, should be periodically reviewed and evolve to address any procedural challenges and facilitate efficient cloud adoption.
COORDINATING BODY FOR CLOUD ADOPTION	Establishing a dedicated agency, such as *Jabatan Digital Negara*, will drive cloud adoption in the public sector, coordinate skills development across public agencies, and encourage ministries to develop cloud transformation roadmaps aligned with the goals under the NCCP. The agency will also facilitate skills training with private sector expertise, improving digital capabilities across government.
CYBERSECURITY AWARENESS	Promotes public education on best practices for securing cloud services, emphasising the importance of strong passwords, multi-factor authentication, and other essential security measure.

Private Sector	
INNOVATION AND CAPACITY BUILDING	CSPs should foster innovation and support capacity-building initiatives, such as training programs and hackathons, to encourage cloud technology adoption.
REGULATORY COMPLIANCE AND SECURITY	CSPs must prioritise compliance with national and international regulations and implement strong governance frameworks.
SERVICE QUALITY AND RELIABILITY	Providers are responsible for maintaining high service standards, transparency in service quality, uptime commitments and support services.
SUPPORT FOR MICRO, SMALL AND MEDIUM ENTERPRISES (MSME) CLOUD ADOPTION	CSPs, in collaboration with government agencies, should consider incentives such as subsidised tools and grants to encourage cloud adoption among MSMEs.
STANDARDISATION AND ADVOCACY	The private sector is encouraged to promote cloud computing standards and actively engage in policy advocacy, contributing to the development of a supportive regulatory framework.

Citizens	
AWARENESS AND EDUCATION	Citizens should participate in initiatives to improve digital literacy and understand both the benefits and risks of cloud technologies.
INFORMED DECISION-MAKING	Individuals are encouraged to evaluate CSPs based on their data security practices, privacy policies, and service reliability.
CYBERSECURITY AND DATA PROTECTION	Citizens must adopt good cybersecurity habits, such as using strong passwords, enabling multi-factor authentication and regularly updating their devices and software. They must also understand their data privacy rights and exercise them responsibly to safeguard personal information.

4.4 Collaboration And Consumer Protection

Collaboration with CSPs and consumer protection mechanisms are important to maintain a secure and transparent cloud ecosystem.

INDUSTRY COLLABORATION MECHANISMS	Public-Private Partnerships (PPPs), industry forums, standards committees and technical committees are essential for fostering collaboration between the government, CSPs and industry bodies. These collaborative efforts aim to address regulatory requirements and data security challenges effectively. CSPs are also encouraged to partner with sector-specific regulators to develop tailored security guidelines, such as the Risk Management in Technology (RMiT) policy developed by Central Bank of Malaysia for the financial sector.
CONSUMER PROTECTION	A strong consumer protection framework safeguards user interests and enhances the trustworthiness of CSPs, fostering consumer confidence and loyalty, and helping CSPs gain a competitive edge in the market. Key elements include: • **Dispute Resolution Process** - Consumers must have accessible channels to file complaints with CSPs, including clear escalation pathways if initial concerns are not resolved. • **Compensation and Remedies** - CSPs are required to provide appropriate remedies for incidents which may include financial compensation, service credits, or identity protection services, depending on the severity of the event. • **Transparency and Reporting** - CSPs are recommended to notify affected users of significant incidents and provide transparency on compensation measures offered.

PART 5: TRACKING PROGRESS

To ensure that the NCCP remains relevant and effective, a robust framework for tracking progress and incorporating feedback is essential. This section outlines the mechanisms for measuring performance, gathering stakeholder input, and periodically reviewing and updating the policy.

5.1 Performance Tracking and Milestones

Performance tracking mechanisms will measure progress across different sectors using key milestones such as:

Cloud Adoption Rates	Service Efficiency Improvements	Economic Impact	Environmental Impact
Metrics to evaluate cloud service adoption rate.	Indicators to measure improvements in service delivery and operational efficiency.	Metrics to gauge the economic benefits, including cost savings and increased competitiveness through cloud adoption.	Metrics to assess reductions in carbon footprints and other environmental benefits achieved through cloud services.

Regular reporting will monitor progress, identify bottlenecks in implementation, and recalibrate strategies to ensure that milestones met effectively.

5.2 Feedback and Policy Reviews

Stakeholder feedback is critical to refining the NCCP and ensuring its continued relevance. Feedback mechanisms include:

BIENNIAL POLICY REVIEWS	Comprehensive reviews conducted every two years to evaluate the NCCP's impact across all sectors - government agencies, private businesses (especially SMEs), academia and citizens. The review will consider emerging technological trends in cloud computing and feedback from stakeholders.
STAKEHOLDER FEEDBACK MECHANISMS	Formal channels such as surveys, public forums, and direct input through online platforms.
PUBLIC CONSULTATION	Major policy updates will involve public consultations to ensure inclusivity across all stakeholders. Targeted focus groups will address issues faced by specific segments (e.g., SMEs, rural communities, government agencies).
INTERIM UPDATES	Interim updates may be issued to address significant technological or regulatory changes or respond to specific stakeholder concerns.
DYNAMIC AND ADAPTIVE POLICY FRAMEWORK	The NCCP is a living document designed to evolve with technological advancements, regulatory updates, and stakeholder needs. Its adaptability ensures that the policy remains aligned with best practices, security standards, and emerging global trends through ongoing reviews and interim updates.

5.3 Compliance Monitoring and Reporting

Adherence to NCCP standards is essential for maintaining operational excellence. Mechanisms include:

Continuous Compliance Checks	Key Performance Indicators (KPIs)	Incident Reporting Protocols
Regular audits to assess CSP and public sector compliance with data protection, cybersecurity, and performance standards.	Metrics for service uptime, adoption rates, and improvements in operational efficiency.	CSPs must report incidents involving data breaches, operational failures, or cybersecurity threats to regulators to ensure swift mitigation.

5.4 Risk Management and Mitigation Plan

A structured risk management plan is necessary to address potential challenges in cloud adoption and implementation:

Risk Identification	Mitigation Strategies	Escalation Processes
Regular risk assessments to identify potential data breaches, regulatory changes, or technological disruptions.	Proactive measures to minimise the impact of identified risks, including contingency planning and incident response protocols.	Mechanisms for resolving critical risks promptly to minimise disruptions to business or government services.

5.5 Capacity Building and Incentives

Capacity building is essential to equip stakeholders with the skills needed for effective cloud adoption. Key initiatives include:

Training and Workshops	Incentives for Adoption	Public-Private Partnerships (PPP)	Focus on Underserved Regions
Regular sessions for public and private sector stakeholders to enhance their understanding of cloud technologies and best practices.	Selective incentives, such as tax breaks or grants, may be considered to promote cloud adoption by making cloud solutions more affordable.	Collaborations between the public and private sectors will facilitate the sharing of resources, expertise, and best practices.	Specialised training and infrastructure grants will target rural and underserved regions to ensure equitable capacity building.

PART 6: CALL TO ACTION – THE PATH FORWARD FOR A RESILIENT CLOUD ECOSYSTEM

6.1 Whole-of-Nation

To secure Malaysia's position as a leading global player in the cloud computing space, all stakeholders must come together in a collective effort. Government agencies, the private sector, CSPs, academia, and citizens all have a role to play in implementing the initiatives outlined in this policy. Key actions include:

Government Agencies

Accelerate the integration of cloud technologies into public services, streamline regulatory approvals, and foster an environment conducive to innovation.

Private Sector

Embrace cloud solutions to drive business growth, improve operational efficiency, and collaborate with the government to identify opportunities for joint ventures and partnerships, and promote innovation across sectors.

Cloud Service Providers

Ensure adherence to the highest standards of data privacy, security, and compliance, while providing accessible solutions that cater to the diverse needs of both public and private sectors.

Academia and Research Institutions

Develop curricula focused on cloud technologies and research initiatives that equip students and professionals with future-ready skills necessary for Malaysia's digital transformation.

Civil Society & Citizens

Engage in dialogues about cloud adoption, raise awareness on data privacy and inclusivity, and ensure that the needs of vulnerable and underserved communities are not overlooked.

6.2 Building Resilience in the Cloud Ecosystem

As Malaysia develops its cloud ecosystem, building resilience is a key priority, to ensure that cloud infrastructure is capable of withstanding and quickly recovering from disruptions:

Disaster Recovery and Redundancy

Implementing measures such as Disaster Recovery as a Service (DRaaS), data redundancy protocols, and failover capabilities across critical infrastructure – both private and public - to ensure uninterrupted access during emergencies.

Cybersecurity

Establish robust cybersecurity frameworks that safeguard against cyber threats while ensuring compliance with national cyber security law.

Operational Continuity

Ensure critical infrastructure remains operational during emergencies by aligning resilience strategies with national security priorities.

Ongoing Monitoring of Emerging Risks

Establish structured frameworks for regular risk assessments and reviews to address vulnerabilities in emerging technologies like AI and IoT.

AI and IoT Security Guidelines

Ensure algorithmic transparency, robust data protection for IoT devices, and compliance with international IoT security standards.

6.3 International Collaboration

Malaysia's cloud strategy will align with international standards and best practices, such as ISO/IEC frameworks while fostering partnerships with global technology leaders, enabling knowledge transfer and encouraging innovation. These collaborations will drive innovation through knowledge exchange while positioning Malaysia as a competitive player in the global cloud landscape. International partnerships should also include sharing best practices in cybersecurity and resilience to strengthen Malaysia's preparedness for cross-border challenges in cloud computing.

Knowledge Transfer

Collaborate with global cloud leaders to adopt cutting-edge technologies and best practices.

Cybersecurity Resilience

Partnerships will also include sharing of best practices in cybersecurity and disaster preparedness to bolster cross-border resilience in cloud computing.

Global Standardisation

Work to harmonise Malaysia's regulatory frameworks with internationally recognised standards to facilitate seamless cross-border operations for cloud operations.

6.4 Inclusivity and Digital Literacy

To fully harness the potential of cloud computing, efforts must focus on increasing digital literacy among citizens and closing the digital divide:

Digital Literacy Initiatives

Developing digital literacy programs to empower all citizens to use cloud-based services confidently and effectively.

Equitable Access

Ensure equitable access through targeted investments in rural infrastructure expansion while promoting affordable cloud solutions across underserved regions.

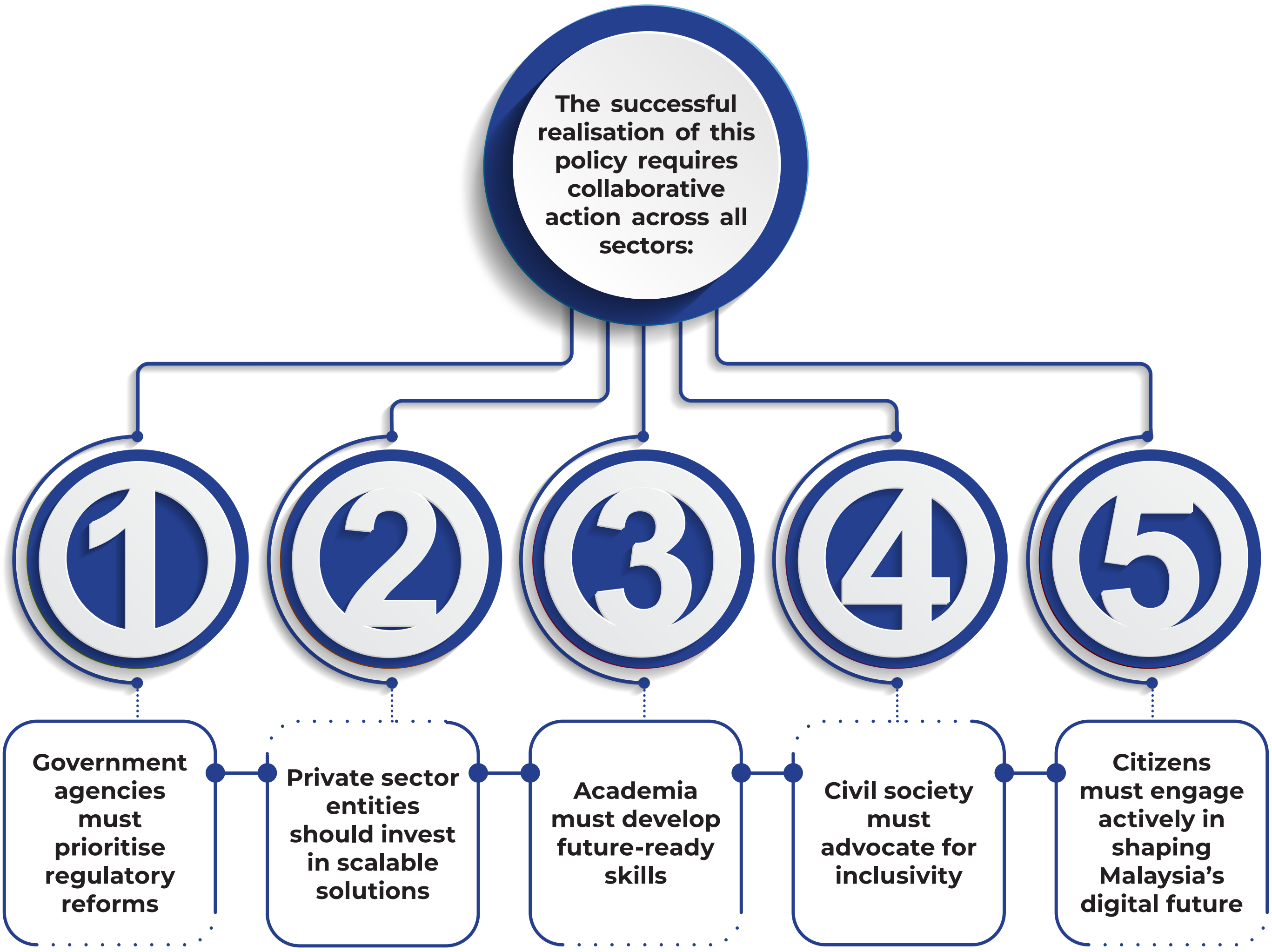
Engagement With Vulnerable Communities

Tailor digital literacy programs to include marginalized groups, ensuring they have equal opportunities to benefit from Malaysia's digital transformation.

Awareness Campaigns

National campaigns promoting awareness of data privacy, cloud benefits, and security risks will be launched to build trust and confidence among citizens.

6.5 Conclusion



The successful realisation of this policy requires collaborative action across all sectors:

Government agencies must prioritise regulatory reforms

Private sector entities should invest in scalable solutions

Academia must develop future-ready skills

Civil society must advocate for inclusivity

Citizens must engage actively in shaping Malaysia's digital future

By aligning efforts toward building a resilient ecosystem through continuous learning and adaptation, Malaysia can unlock the full potential of cloud computing, driving economic growth while promoting sustainable digital inclusivity.

Living Document

The NCCP will continue to be reviewed and updated regularly to reflect changes in the global cloud landscape. This ongoing commitment to adaptation ensures Malaysia remains proactive, driving competitiveness and fostering inclusivity. Through collective effort, continuous learning, and proactive adaptation, the NCCP will empower Malaysia to lead in cloud innovation, positioning the country as a premier global cloud hub for a thriving, sustainable, and inclusive digital economy.

APPENDIX A : CLOUD MODELS AND SERVICE LAYERS

This section provides an in-depth overview of the cloud models and service layers that are fundamental to understanding the cloud ecosystem.

A1 Cloud Deployment Models

The NCCP recognises 5 kinds of deployment models for cloud services:

NO.	DEPLOYMENT MODEL	DEFINITION	USE CASE EXAMPLE
1	PUBLIC CLOUD	Scalable, cost-effective, and accessible cloud services to a wide range of users, including businesses, government agencies, and individual citizens.	**a) Startups and SMEs** Cost-effective for organisations with limited IT budgets. **b) Development and Testing** Ideal for spinning up environments quickly for short-term use. **c) Big Data and Analytics** Public clouds provide powerful processing capabilities for data analysis. **d) Disaster Recovery** Affordable and scalable off-site backups. **e) Affordable and scalable off-site backups** Ability to handle variable traffic and seasonal demand spikes.
2	PRIVATE CLOUD	Secure, dedicated, and customisable cloud services for specific organisations, including government agencies, large enterprises, and institutions with sensitive data requirements, supporting enhanced data security, regulatory compliance, and operational efficiency.	**a) Regulated Industries** (e.g., Finance, Healthcare, Government) - Industries with strict data compliance and security regulations often prefer private clouds to ensure adherence to certain specific standards. **Example**: A hospital uses a private cloud for storing sensitive patient records and running AI algorithms to analyse health data while maintaining data privacy. **b) Highly Sensitive Data Workloads** - Private clouds provide greater isolation and security, protecting intellectual property or trade secrets. **Example** : A defense contractor processes classified government data on a private cloud to ensure maximum security. **c) Customisable Enterprise Applications** - Private clouds allow organisations to configure infrastructure to meet the unique requirements of specific applications. **Example** : A financial services firm deploys customised trading applications on a private cloud for optimal performance and regulatory compliance. **d) Mission-Critical Workloads** - ensure higher availability, dedicated resources, and better control for workloads that must operate without interruption. **Example**: An airline uses a private cloud to manage real-time flight scheduling and ticketing systems, ensuring reliability.

NO.	DEPLOYMENT MODEL	DEFINITION	USE CASE EXAMPLE
			e) **Research and Development (R&D)** - Private clouds support compute-intensive tasks like simulations, testing, and machine learning model training, with full control over resources. **Example**: A pharmaceutical company runs drug discovery simulations on a private cloud to secure sensitive research data. **Legacy System Integration** - Many legacy systems are challenging to migrate directly to public clouds, so private clouds provide a controlled environment for integration.
3	**HYBRID CLOUD**	Combines the benefits of both public and private clouds for a balanced approach to offer flexible, scalable, and secure cloud solutions. It supports diverse computing needs, enabling seamless integration and data portability across different cloud environments.	a) **Dynamic Workloads (Cloud Bursting)** - An e-commerce company uses a private cloud for daily operations and a public cloud during holiday sales to handle increased traffic. b) **Regulatory Compliance** - A bank stores customer financial data in a private cloud but uses public clouds for running analytics on anonymized data. c) **Backup and Disaster Recovery** - A hospital stores patient records in a private cloud but backs up data to a public cloud for disaster recovery. d) **Development and Testing** - A software company tests new features in the public cloud to save costs, then deploys to a secure private environment. e) **Big Data and Analytics** - A logistics company analyses shipping data in the public cloud while maintaining customer details in a private cloud. f) **Gradual Cloud Migration** - A manufacturing firm migrates legacy ERP systems to a private cloud while integrating with public cloud analytics tools. g) **IoT and Edge Computing** - A smart city collects traffic data locally and uses a public cloud to analyse patterns for optimisation.
4	**COMMUNITY CLOUD**	A shared infrastructure tailored for specific community users, often with shared concerns such as mission, security, or compliance.	a) **Government Agencies** - Different government departments (e.g., healthcare, public safety, transportation) can share a cloud to securely store and process citizen data while adhering to regulatory policies. **Example**: Local governments collaborate on a community cloud to manage citizen services and share disaster recovery solutions. b) **Healthcare Organisations** - Hospitals, clinics, and healthcare providers can store sensitive patient data on a community cloud, ensuring compliance with healthcare regulations. **Example** : A group of hospitals shares a cloud for secure patient record storage and data analysis for medical research. c) **Educational Institutions** - Universities and research institutes can share infrastructure for collaborative research and data storage. **Example** :A consortium of universities uses a community cloud to run academic research programs and share libraries of educational resources.

NO.	DEPLOYMENT MODEL	DEFINITION	USE CASE EXAMPLE
			d) Financial Institutions - Banks and financial organisations can collaboratively use a community cloud to develop and deploy industry-standard applications and comply with financial regulations. **Example** :Regional credit unions use a community cloud to jointly manage customer data and fraud detection systems. **e) Non-Profit Organisations** - Non-profits with similar missions can share resources to reduce costs while achieving their objectives. **Example** : Environmental organisations use a community cloud to manage and analyse climate data for global sustainability initiatives. **f) Research Collaborations** - Scientists and researchers from various organisations can share infrastructure to run simulations and analyse data. **Example** : A global community cloud supports joint research in astrophysics, sharing computing power for telescope data processing.
5	**MULTI-CLOUD**	Multi-cloud deployment models involve using multiple cloud services from different providers to improve resilience, flexibility, and avoid vendor lock-in. This approach enhances redundancy by allowing organisations to maintain service availability during outages, optimises performance by leveraging the strengths of various cloud platforms, and ensures compliance with data sovereignty regulations by distributing data across regions.	**a) Disaster Recovery and High Availability** - Multi-cloud can be used to build redundancy for mission-critical systems, ensuring uptime even if a single provider fails. **b) Compliance and Governance** - Organisations can store data in specific regions to meet regulatory requirements, using cloud providers with local compliance certifications. **c) Cost Optimisation** - Applications can run on the most cost-efficient provider based on workload characteristics. **d) Performance Optimisation** - Using providers close to the end-user can improve latency and overall performance.

A2 Cloud Deployment Models

The NCCP recognises six kinds of internationally well-known deployment models for cloud services:

NO	CLOUD SERVICE MODEL	DEFINITION
1	**INFRASTRUCTURE AS A SERVICE (IaaS)**	Provides on-demand virtualised computing resources such as virtual machines, storage, and networking. Supports scalability, cost-efficiency, and flexibility.
2	**PLATFORM AS A SERVICE (PaaS)**	Offers a platform for developing, running, and managing applications without the complexity of maintaining underlying infrastructure.
3	**SOFTWARE AS A SERVICE (SaaS)**	Delivers software applications over the internet on a subscription basis, supporting remote work and flexible arrangements.
4	**STORAGE AS A SERVICE (STaaS)**	Offers scalable, on-demand storage solutions that allow organisations to manage data without physical infrastructure investments.
5	**DISASTER RECOVERY AS A SERVICE (DRaaS)**	DRaaS plays a critical role in Malaysia's National Cloud Computing Policy, providing cloud-based disaster recovery solutions to ensure quick recovery of IT systems and data during disasters. This service minimises downtime and data loss, promoting resilience, reliability, and continuity for both government and private sectors.
6	**XaaS: EVERYTHING AS A SERVICE XaaS, OR "ANYTHING AS A SERVICE**	Refers to a range of IT solutions delivered over the internet, allowing organisations to access and utilise technology without owning or managing the underlying infrastructure. This model transforms IT service delivery by enhancing agility, reducing costs, and improving operational efficiency through cloud-based solutions. As businesses increasingly adopt XaaS, it is crucial to align these services with broader organisational goals and strategies to ensure a cohesive approach to digital transformation

APPENDIX B : RELEVANT LAWS AND STANDARDS

This appendix summarises the key laws, certifications, standards, and guidelines governing cloud computing in Malaysia. It is organised into 5 sections: Legal and Regulatory Framework, Certifications and Standards, Sector-Specific Guidelines, Global Cloud Security Frameworks, and Emerging Guidelines.

B.1 LEGAL AND REGULATORY FRAMEWORK

This section outlines the key legal instruments governing cloud computing in Malaysia:

LAW/ACT	APPLICABILITY	PURPOSE
PERSONAL DATA PROTECTION ACT 2010 *[ACT 709]*	Processing of personal data in commercial transaction, excluding Federal and State Government	Regulates the processing of personal data in commercial transactions which includes: a) Obligations on Data Controller to comply with seven (7) Personal Data Protection Principle and Data Processor (e.g., CSPs) under the Security Principle, requiring them to implement appropriate security measures to protect personal data they process on behalf of Data Controllers; b) Mandatory appointment of a Data Protection Officer (DPO) responsible for ensuring compliance with the Act; c) Mandatory notification of personal data breaches to the Personal Data Protection Commissioner; d) Obligations on Data Controller to respond with data subject rights including data portability rights allowing data subjects to request their personal data be transferred from one Data Controller to another. e) The guidelines set out under Guideline for Appointment of Data Protection Officer and Guideline for Data Breach Notification.
COMMUNICATIONS AND MULTIMEDIA ACT 1998 *[ACT 588]*	Cloud service providers offering PaaS or IaaS services	Requires CSPs providing Platform as a Service ('PaaS') or Infrastructure as a Service ('IaaS') to obtain an Application Service Provider Class License ('ASP (C)'). The licensing framework for cloud service does not impose licensing requirement for a person that is providing Software as a Service ('SaaS') only. Reference: Information Paper on Regulating Cloud Services (updated as of 30 September 2024)
CYBER SECURITY ACT 2024 *[ACT 854]*	National Critical Information Infrastructure (NCII) entities	An Act to enhance the national cyber security by providing for the establishment of the National Cyber Security Committee, duties and powers of the Chief Executive of the National Cyber Security Agency, functions and duties of the national critical information infrastructure sector leads and national critical information infrastructure entities and the management of cyber security threats and cyber security incidents to national critical information infrastructures, to regulate the cyber security service providers through licensing, and to provide for related matters.

OFFICIAL SECRETS ACT 1972 *[ACT 88]*	Government agencies, CSPs handling classified data	Prohibits unauthorised access, disclosure, and handling of classified government information that is considered as secret for the interest and sake of national security.
DATA SHARING ACT 2025 *[ACT 864]*	Public sector, including agencies	Regulates the sharing of data between all public sector entities (intra-government).
COMPETITION ACT 2010	CSPs, telecoms, cloud market players	Prohibits anti-competitive practices such as abuse of dominant market position. It promotes fair access to market infrastructure and prevents monopolistic behaviour that could harm smaller CSPs or startups.
THE PUBLIC SECTOR AI ADAPTATION GUIDELINE	Public sector	To ensure responsible and ethical AI adoption, promote efficiency and effectiveness in AI technology and innovation among civil servants.
PUBLIC SERVICE CIRCULAR LETTER (PKPA) NUMBER 1 OF 2021: PUBLIC SECTOR CLOUD COMPUTING SERVICES POLICY	Public Sector	Provide a framework and guidelines for the adoption and implementation of cloud computing services within the Malaysian public sector. This ensures a consistent and strategic approach across all government agencies.
PUBLIC SERVICE CIRCULAR LETTER (SPA) NUMBER 2 OF 2021 VERSION 2.0: GUIDELINES FOR INFORMATION SECURITY MANAGEMENT THROUGH CLOUD COMPUTING IN THE PUBLIC SERVICE	Public Sector	to provide guidelines for managing information security when utilising cloud computing services within the Malaysian public sector.
CIRCULAR LETTER 2.6: PROCUREMENT OF PUBLIC SECTOR CLOUD COMPUTING SERVICES.	Public Sector	to provide guidelines and procedures for the procurement (acquisition) of cloud computing services by the Malaysian public sector.

B.2 CERTIFICATIONS, STANDARDS, AND SUSTAINABILITY

This section lists key certifications and standards relevant to cloud computing in Malaysia:

CLOUD CERTIFICATIONS AND STANDARDS	
CERTIFICATION/STANDARD	**PURPOSE**
ISMS CERTIFICATION (ISO/ IEC 27017)	ISO 27017 is essentially an extension of ISO 27001, offering additional guidance for both cloud service providers and customers on cloud-specific security practices guidelines for implementing information security controls tailored to cloud computing environments.
SOC 1, SOC 2, SOC 3	Financial reporting and operational security standards for data centres.
PCI DSS	Ensures secure handling of payment data in cloud environments.
ANSI/TIA-942	Telecommunications infrastructure standard for data centres. Covers Data Centre Tier Classification from Tier 1 to Tier 4.
ISO/IEC 27002:2022	Information security management guidelines covering cybersecurity and privacy controls. Updated version from 2022 provides enhanced controls for cloud environments.
ISO/IEC 17788:2014	Provides an overview of cloud computing concepts and terminology to ensure common understanding across stakeholders.
ISO/IEC 27001:2022	Provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS), and has been updated with new requirements for managing information security risks in cloud environments.
ISO/IEC WD TR 3445	Working draft standard still under development for auditing cloud services. Provides guidelines for conducting audits in cloud environments once finalised.
ISO/IEC 30134-1:2018	Energy efficiency guidelines for computing systems in data centres – Part 1: Overview and General Requirements for Energy Efficiency Metrics in IT environments.
ETSI EN 303 470	Defines energy efficiency metrics for servers used in cloud environments.

SUSTAINABILITY AND GREEN CLOUD COMPUTING	
STANDARD	**PURPOSE**
ISO/IEC TR 30132-1:2016	Provides guidelines for evaluating energy effectiveness in cloud environments.
ISO/IEC 30134-2:2018	Defines Power Usage Effectiveness (PUE), a key metric for measuring energy efficiency in data centres by comparing total facility energy usage to IT equipment energy usage.
ISO/IEC DIS 30134-6:2023	Defines the Energy Reuse Factor (ERF), which measures how much energy from a data centre is reused for other purposes such as heating other facilities or processes.
ISO/IEC CD 30134-7 PART 7: COOLING EFFICIENCY RATIO (CER)	Provides metrics on cooling efficiency within data centres by measuring how effectively cooling systems are used relative to IT equipment energy consumption.
ISO/IEC CD 30134-8 PART 8: CARBON USAGE EFFECTIVENESS (CUE)	Measures carbon emissions relative to IT equipment energy consumption within a data centre environment as part of sustainability efforts.
ISO/IEC CD 30134-9 PART 9: WATER USAGE EFFECTIVENESS (WUE)	Measures water consumption relative to IT equipment energy consumption within a data centre environment as part of sustainability efforts.
ISO 50001 – ENERGY MANAGEMENT SYSTEM	Provides a framework for establishing energy management systems aimed at improving energy performance in organisations using cloud infrastructure.

B.3 SECTOR-SPECIFIC GUIDELINES

Financial Sector

a) *Risk Management in Technology (BNM)*: Strengthens technology risk management for financial institutions through governance frameworks that address cybersecurity risks related to cloud usage in the financial sector.

b) *Information, Communications and Digital Sector: The Information and Network Security Guidelines (INSG) introduced by the Malaysian Communications and Multimedia Commission (MCMC) aim to strengthen cybersecurity within Malaysia's communications and multimedia industry.*

B.4 GLOBAL CLOUD SECURITY FRAMEWORKS

This section highlights global frameworks relevant to cloud security:

FRAMEWORK	PURPOSE
CLOUD SECURITY ALLIANCE (CSA)	Provides best practices for cloud security; CSA's Cloud Controls Matrix (CCM) helps align with international standards while ensuring compliance with local regulations like PDPA and CMA. CSPs can use CSA STAR certification as part of their compliance efforts under Malaysia's Cybersecurity Act when providing services to critical sectors or government agencies.
NIST CLOUD STANDARDS ROADMAP – SPECIAL PUBLICATION SERIES SP500-29X	Offers guidance on standardisation and security; provides a framework for secure cloud adoption through interoperability standards and risk management methodologies that can be adapted locally by CSPs operating within regulated sectors like finance or telecommunications.
NIST SPECIAL PUBLICATION SP500-316 – FRAMEWORK FOR CLOUD USABILITY	Focuses on usability aspects of cloud computing services by providing best practices on how organisations can ensure that their use of cloud services meets user needs efficiently while maintaining security controls.
NIST SPECIAL PUBLICATION SP800-144 – GUIDELINES ON SECURITY & PRIVACY IN PUBLIC CLOUD COMPUTING	Provides detailed guidelines on managing security risks when using public cloud services by addressing issues such as shared responsibility models between CSPs and customers.
ENISA CLOUD STANDARDS & SECURITY GUIDELINES	Offers guidance on securing cloud services across the European Union by addressing key risks such as data protection, legal compliance, operational resilience, and incident response frameworks for CSPs operating globally or within Europe.
FEDRAMP (U.S.)	A U.S.-based program ensuring security compliance for CSPs handling government data.
HIPAA COMPLIANCE STANDARDS	U.S.-based Health Insurance Portability & Accountability Act which sets strict requirements around protecting health-related personal information when using cloud services—relevant for healthcare organisations using CSPs.

B.5 Emerging Guidelines

This section outlines upcoming guidelines being developed by the Personal Data Protection Department that are expected to impact CSPs:

a) ***Personal Data Protection Standard*** – A new standard replacing the existing one from 2015

b) ***Guidelines on Data Portability***

c) ***Guidelines on Privacy Impact Assessments***

d) ***Guidelines on Privacy by Design***

e) ***Practical Guide: AI Governance and Ethics***

f) ***Framework for Sustainable Data Centre Industry Development in Malaysia***