PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA

MYSEAL

SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA

BAHAGIAN POLISI, PERUNDANGAN DAN KESEDARAN

MYSEAL

- Serves as a comprehensive resource for the implementation of cryptographic algorithms in information security systems, providing guidance and references for users.
- Aims to enhance the protection and security of classified information transmitted electronically in Malaysia.

MYSEAL CATEGORIES

Algoritma Kriptografi Sedia Ada (AKSA)

Cryptographic algorithms that have been published in recognized standards or have undergone thorough evaluation in established cryptographic algorithm projects.

Algoritma Kriptografi Baharu (AKBA)

New cryptographic algorithms that have not yet been published in recognized standards or widely adopted in the cryptographic community

AKSA CATEGORIES

AKSA MySEAL 2.0 Approved

Algorithms that have met high standards of security and compliance, approved for secure digital applications in Malaysia.

AKSA MySEAL 2.0 Neutral

Algorithms that are considered secure but may not meet all the criteria for the "Approved" category.

AKSA MySEAL 2.0 Legacy

Older algorithms that are still in use but are not recommended for new applications due to potential security vulnerabilities.

PURPOSES OF MYSEAL

✅ Enhances digital security for government, businesses, and individuals.

✅ Provides secure authentication for online transactions.

✅ Protects sensitive data with encryption.

✅ Ensures compliance with Dasar Kriptologi Malaysia (DKM).

✅ Enables secure communication & cross-border digital services.

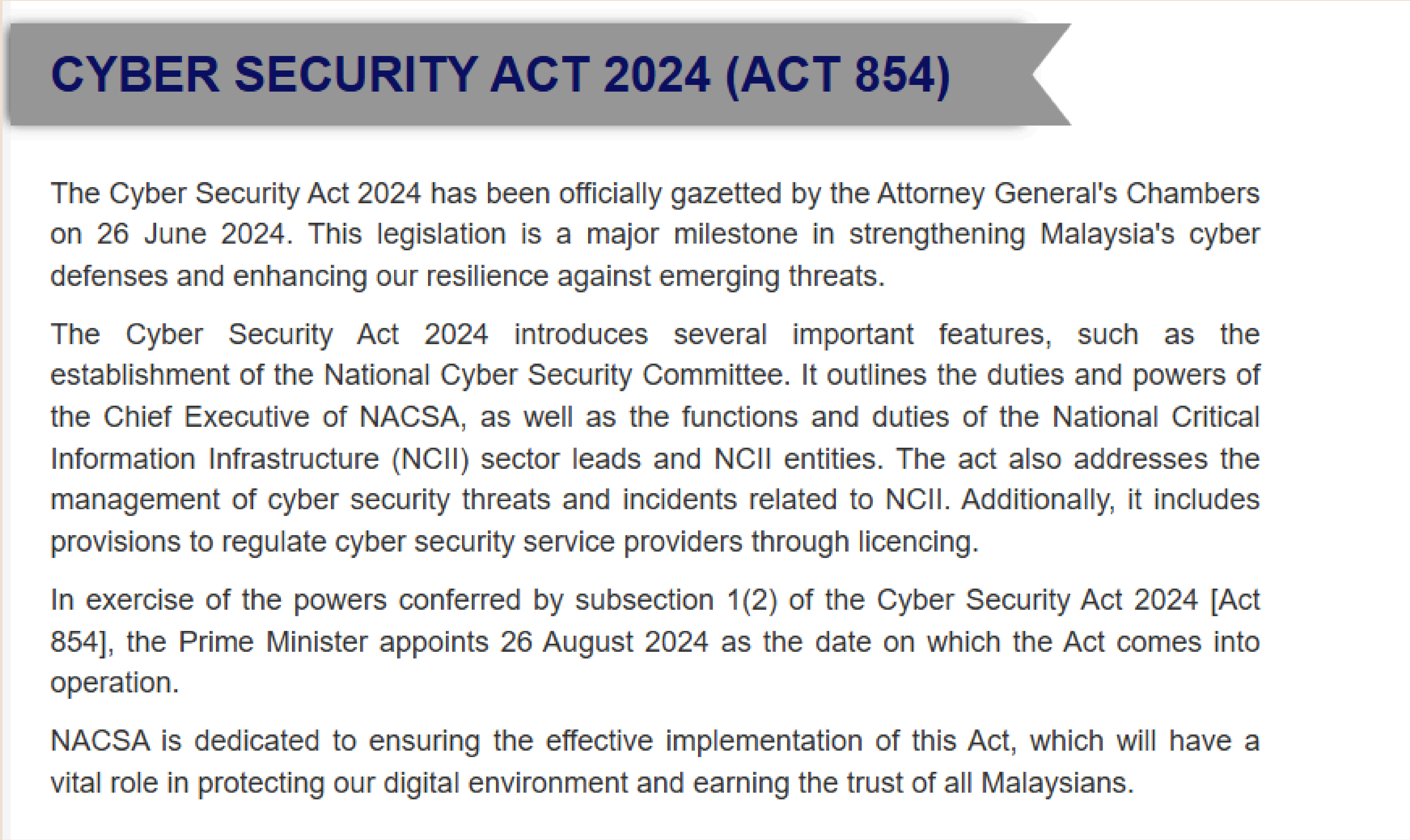
PURPOSES OF AKSA

✅ Protects legacy systems using traditional encryption.
✅ Ensures compliance with cybersecurity standards.
✅ Secures digital transactions & communications.
✅ Acts as a bridge before transitioning to PQC.

PURPOSES OF AKBA

✅ Prepares Malaysia for the Post-Quantum era.
✅ Introduces quantum-resistant cryptographic standards.
✅ Ensures long-term data security against future threats.
✅ Supports secure digital transformation (IoT, blockchain, cloud security, AI).

CYBERSECURITY ACT 2024



CYBER SECURITY ACT 2024 (ACT 854)

The Cyber Security Act 2024 has been officially gazetted by the Attorney General's Chambers on 26 June 2024. This legislation is a major milestone in strengthening Malaysia's cyber defenses and enhancing our resilience against emerging threats.

The Cyber Security Act 2024 introduces several important features, such as the establishment of the National Cyber Security Committee. It outlines the duties and powers of the Chief Executive of NACSA, as well as the functions and duties of the National Critical Information Infrastructure (NCII) sector leads and NCII entities. The act also addresses the management of cyber security threats and incidents related to NCII. Additionally, it includes provisions to regulate cyber security service providers through licencing.

In exercise of the powers conferred by subsection 1(2) of the Cyber Security Act 2024 [Act 854], the Prime Minister appoints 26 August 2024 as the date on which the Act comes into operation.

NACSA is dedicated to ensuring the effective implementation of this Act, which will have a vital role in protecting our digital environment and earning the trust of all Malaysians.

PURPOSES OF CYBERSECURITY ACT

✅ Protects national security from cyber threats.
✅ Safeguards financial & critical infrastructure from cyberattacks.
✅ Defines clear cybersecurity regulations for organizations.
✅ Establishes legal enforcement for cybercrime.
✅ Improves cyber incident response & crisis management.
✅ Promotes cybersecurity innovation & awareness.

BENEFITS OF CYBERSECURITY ACT

- ✅ Increased cybersecurity preparedness.
- ✅ Better governance & regulation.
- ✅ Protection of national security.
- ✅ Improved trust in digital services.
- ✅ Stronger public-private collaboration.

IMPACTS OF CYBERSECURITY ACT

- ✅ National security enhancement.
- ✅ Economic stability
- ✅ Legal accountability.
- ✅ Innovation & growth.
- ✅ Increase public awareness.

RISK

WHAT IS RISK?

Impact of uncertainty on goals

RISK MANAGEMENT

- Process of identifying, assessing, and controlling risks that may affect an organization's ability to achieve its objectives.
- Determine the impact and possibility of risks, creating plans to reduce harm, and keeping an eye on how well measures are working.
- To minimize the potential negative impacts of risks while maximizing the opportunities.
- Critical for organizations across industries to protect assets, reputation, and growth potential.

RISK CAUSES

Category	How It Occurs	Consequences
Cybersecurity Threats	Cyberattacks can lead to data breaches	Data loss and loss of customer trust
Regulatory Changes	New laws can impact organizational operations	Increased compliance costs or operational restrictions
Economic Conditions	Economic downturns can reduce profitability	Cost-cutting measures or layoffs
Operational Failures	Equipment breakdowns can slow down operations	Production disruptions and higher maintenance costs
Technological Failures	Outdated or malfunctioning systems can affect business processes	Productivity loss and system downtime

RISK IMPACTS

Category	Description	Example
Health & Safety	Related to location, lifestyle, occupation, or activity	World war affecting human safety
Quality of Life	Affects nations, cities, communities, organizations, and individuals	Buying a house that determines living standards
Financial	Impacts revenue, costs, and expenses	Lost revenue or increased operational costs
Time	Delays that affect schedules or projects	Construction project delays
Reputation	Related to social factors and public perception	Scandals damaging brand image

POTENTIAL RISKS IF PQC FAILS

Operational Risk	Business Risk	Technical Risk	Financial Risk
Sensitive data breach	Loss of user trust	Algorithm weaknesses	Recovery & data remediation costs
Service disruption	Legal & compliance implication	Dependence on legacy system	Investment losses
Integration errors	Reputation damage	Maintenance & replacement costs	Lawsuits & insurance claims

QUANTUM RISK ASSESSMENT

The quantum weakness of the cryptography that is in use on a system/application level.

The expected impact of a quantum attack on the system.

The estimated time and effort required to migrate to post-quantum cryptography.

METHODS FOR QUANTUM RISK ASSESSMENT

Cryptographic Inventory Audit

- List all cryptographic algorithms used in a system
- Identify which ones are vulnerable to quantum attacks.

Risk Classification

- High Risk
- Medium Risk
- Low Risk

PQC Migration Plan

- Select appropriate PQC algorithms.
- Test their effectiveness and compatibility with existing systems.
- Implement a phased transition to prevent operational disruptions.

WHY QUANTUM RISK ASSESSMENT IMPORTANT?

- Ensures national and organisational security against quantum attacks
- Prevent data violations and large-scale cyberattacks
- Supports a smooth transition to PQC without disrupting operations

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

GOVERNMENT

ASSETS	DATA	RISK
Government websites, portals and databases	National security data	Decryption of classified military/police data
	Legal documents	Digital signature forging to alter law or contract
National identity databases	National identification number	Decryption of stored national ID numbers

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

BANKING AND FINANCE

ASSETS	DATA	RISK
Payment gateways and financial transaction systems	Credit and debit card details	Interception of card transactions via TLS decryption
ATMs and point-of-scale systems	ATM maintenance logs	Alteration of firmware updates by forging RSA signature
Banking platforms	Customer account information, transaction records	Decryption of customer financial data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

TRANSPORTATION

ASSETS	DATA	RISK
Public transportation networks	Payment and operational data	Decryption of RSA/ECC in payment system and operational data
Port and logistics management systems	Port security logs	Decryption of access control and surveillance data
Traffic management systems and smart traffic lights	Traffic flow data	Decryption of TLS of real-time monitoring & control data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

DEFENSE AND NATIONAL SECURITY

ASSETS	DATA	RISK
National defense command and control systems	National defense strategies	Decryption of ECC/RSA cryptography in military communications
Border control and surveillance systems	Border surveillance data	Decryption of AES-256 or RSA-2048 for encrypting monitoring systems

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

INFORMATION, COMMUNICATION AND DIGITAL

ASSETS	DATA	RISK
Telecommunications network and infrastructure	Network equipment, protocols and routing	Decryption of RSA/ECC, TLS/SSL, IPSec, and VPN for securing the communication channel
Data centers and cloud services	Data storage and backup system	Decryption of AES-256 or ECC used secure stored data and backups

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

HEALTHCARE SERVICES

ASSETS	DATA	RISK
Hospital information systems and electronic health records (EHR)	Patient health records	Decryption of AES-256 or ECC for securing patient health data
Medical devices	Medical device data	Decryption of AES-128/256, RSA or ECC that is used to secure transmitted data between devices

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

WATER, SEWERAGE AND WASTE MANAGEMENT

ASSETS	DATA	RISK
Water distribution and treatment system	Water distribution and treatment data	Decryption of AES-128/256 or RSA/ECC to protect data transmitted between sensors, control systems and management platforms
Waste management and disposal systems	Collection and disposal data	Decryption of AES-128/256 or RSA/ECC used to secure those data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

ENERGY

ASSETS	DATA	RISK
Power generation plants	Energy generation metrics, plant operational statuses, fuel usage and efficiency data	Decryption of AES-256 or RSA-2048 for securing communication between power plants and central monitoring/control systems
Oil and gas infrastructure	Pipeline pressure and flow data, equipment performance logs, exploration and supply chain data	Decryption of AES-256 or RSA-2048 used in securing transmission and distribution line data, voltage levels and operational data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

AGRICULTURE AND PLANTATION

ASSETS	DATA	RISK
Crop monitoring systems	Crop and soil data	Decryption of AES-128 or RSA used for securing sensor data, including crop and soil health metrics
Supply chain and logistics systems	Supply chain data	Decryption of RSA/ECC exposing supply chain routing information, delivery schedules and inventory management data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

TRADE, INDUSTRY AND ECONOMY

ASSETS	DATA	RISK
E-commerce platforms and digital retail systems	Customer login credentials, payment details and transaction histories	Decryption of TLS 1.2/1.3 (RSA/ECC) for securing communication between customers and platforms
Intellectual Property (IP)	Intellectual property data (IP)	Decryption of RSA-2048, AES-256 or ECC used for securing patents, trade secrets and other sensitive IP data

QUANTUM THREAT RISK ASSESSMENT FOR NCII SECTOR

SCIENCE, TECHNOLOGY AND INNOVATION

ASSETS	DATA	RISK
Research and development (R&D) facilities and lab	Research findings	Decryption of RSA-2048, AES-256 or ECC used for securing sensitive research outcomes
	Experimental data	Decryption of RSA-2048, AES-256 used for encrypting raw experimental data, test logs and results from simulations
Technology infrastructure	Technology development logs	Decryption of AES-256 or RSA-2048 used for encrypting technology development logs