

**VIRTUAL INDUSTRY FORUM: PROFESSIONALISM
AND ETHICS 2026**

BUILDING A TRUSTED DIGITAL ECONOMY THROUGH ETHICAL INNOVATION



**IR. DR. MEGAT ZUHAIRY BIN MEGAT TAJUDIN
CHIEF EXECUTIVE
NATIONAL CYBER SECURITY AGENCY (NACSA)**

The Trust Promise

"Trust is not a by-product of the digital economy. It is its infrastructure."

- **Digital Malaysia 2030** - a promise that when citizens share their identity and businesses share their data, they will not be exploited, exposed, or harmed.
- How do we build a digital economy that people are confident enough to adopt at scale?

Ethics in the Age of Digital Trust

01

Governance – deciding who is responsible for what, before something goes wrong.

02

Data – entrusted to us by people. Whoever holds a deposit holds an obligation.

03

Human Accountability – a named human behind every consequential decision.



Malaysia's Governance Foundation

Legal and policy pillars for a trusted digital economy:



Cyber Security Act 2024 [Act 854]

Makes cybersecurity a duty, not a courtesy, for entities operating National Critical Information Infrastructure (NCII).



Cybercrimes Bill 2026

Once in force, replaces the Computer Crimes Act 1997 with a framework fit for today's threats.



Malaysia Cyber Security Strategy 2025–2030

Sets our national direction for protection and resilience.



AI Systems Cybersecurity Framework

Translates high-level security and trust requirements into practical controls across four core pillars: data provenance, red-teaming, algorithmic auditing, and failsafe or kill-switch mechanisms.

Pillar One: Governance

01

Law Sets the Floor

Compliance tells you what you must do.
Regulation will always trail technology, so waiting for a rule to tell us what is right leaves us one step behind the risk.

02

Ethics Sets the Ceiling

Ethics asks what you should do. The professional who says "it is not prohibited" has asked the wrong question.

"Is it safe, is it fair, and would I be comfortable explaining it to the people it affects?"

Three Tests of Good Governance

Ownership

Who is accountable for
cyber and AI risk?

Visibility

Does the board see risk
in plain language?

Readiness

Have you rehearsed
your worst day?

The Standard

A named owner with real authority, regular board-level visibility of cyber and data risk, and a response plan that has actually been tested, not only written.

An incident response plan that has never been tested is not a plan. It is hope.

"Data is a deposit. Whoever holds a deposit holds an obligation."

- In the age of AI, ethics begins in the dataset: where did this data come from, who has touched it, and can it be trusted?

Pillar Two: Data

The Morning After

The hardest ethical moment in cybersecurity is not the attack.

Disclose early, explain plainly, and fix visibly: the organizations that do recover trust fastest.

Conceal, delay, or reframe: an incident becomes a scandal, and a scandal becomes a lasting loss of trust.

If you hold people's data, you answer for it.
And you tell them when you have failed to protect it.

Ethical Data Practice

Data minimization is the cheapest cybersecurity control in existence.



Collect Only What You Need

Data you never collected can never be stolen.



Keep It Only As Long As Needed

Retain data for a defined purpose, then dispose of it securely.



Secure It Like Your Own Family's

Protect every record as though it belonged to someone you love.



Be Honest About How You Use It

Tell people plainly how their data is used, and when protection fails.

Human Accountability

A named human behind every
consequential decision.

Oversight that is meaningful, not a
rubber stamp.

There must always
be the ability to
stop.

Kill switches are
a requirement,
not an option.

*Accountability is a
human quality, and it
must stay with humans.*

Accountability Lives in People

01

Verify Before You Act

A cloned voice can sound exactly like a director asking you to bypass a safety procedure.
Verification must be a habit, not only a control.

02

Safe to Speak Up

A culture that punishes honest errors produces concealed errors, and concealed errors are the ones that become disasters.

"Let me verify this first."

Beyond Your Client

Your standing carries a duty to the public interest, not only to your employer or client.

Bridge-Level Standards

We would never accept a bridge without safety margins. Digital systems carrying people's lives deserve the same.

Professional Duty



“Ethical innovation is steering, not braking”

Trust accelerates adoption.
Build security and ethics in from day one.

The economies that lead in 2030 will be those where people are confident enough to adopt at scale.



Five Shared Commitments

01

Own it – name a person accountable for cyber, data, and AI risk, with real authority.

02

Design it in – build security and ethics into products and processes from day one.

03

Respect the data – collect less, protect more, and be honest when things go wrong.



Five Shared Commitments

NACSA stands ready
as your **partner and
national resource** for
the entire **digital
ecosystem**.

04

Keep humans in charge – ensure meaningful oversight, and never build a system that cannot be stopped.

05

Speak up and share – raise concerns early, and report incidents and share threat information with NACSA and sector peers.



Worthy of Trust

Digital Malaysia 2030 will be judged by whether Malaysians trust what we have built.

Every decision in every organization adds to trust or draws from it.

Let us make it worthy of trust.

Trust takes years to build and moments to lose.

Ethical by design, secure by default, accountable through people.



connect with us:

   @NACSAMalaysia

Terima Kasih | Thank You