Information Security Policy

The Management of NEC Asia Pacific Pte Ltd ("NEC APAC") is fully committed to implementing and reinforcing security and good practices in upholding our NEC APAC Information Security Policy. To this end, we shall vigilantly and diligently consider any potential information security risk in safeguarding our business assets against any potential threats.

NEC APAC firmly believes the preservation of information's confidentiality, integrity and availability through information security management is beneficial to the interests of our customers as well as NEC APAC's operations.

NEC APAC is committed to adhering to all applicable requirements relating to information security as well as continually improving the information security management system.

The framework for setting information security objectives involves deriving the measurements metrics from the obligatory aspects for requirements compliance as well as the identified areas of information security weakness from the following sources:

- Legal and regulatory requirements;
- Contractual security obligations;
- Risk management report; and
- Information security review and audits.

The Management has identified the following information security objectives:

- No more than 3 IS incidents due to human error was reported in a year.
- Ensure 99.95% availability of IT infrastructure (exclude scheduled routine/preventive tasks).
- Installed security applications to detect and stop 95% of malicious codes, applications and attacks.

In the provision for information security assurance, individual business units shall be accountable to align their business processes in meeting the information security objectives established.

This policy applies to NEC APAC and all its activities.

Mr. Takayuki INABA
President & CEO
29 Jul 2024