PRIVACY & SECURITY SUMMIT

Co-Hosted By: DUGA Thai Digital Technology User Group Association

NCSA สกมช

Unified Cloud Security: Simplifying Protection Across Hybrid Environments

Privacy & Security Summit 2025

Thursday, May 29, 2025, 13:00 -15:00

Mayfair Ballroom A (Floor 11) The Berkeley Hotel Pratunam, Bangkok

พันตำรวจโท ดร. นรินทร์ เพชรทอง

ผู้อำนวยการฝ่ายฝึกซ้อมและทดสอบสถานะความพร้อม

CISSP CC

Agenda

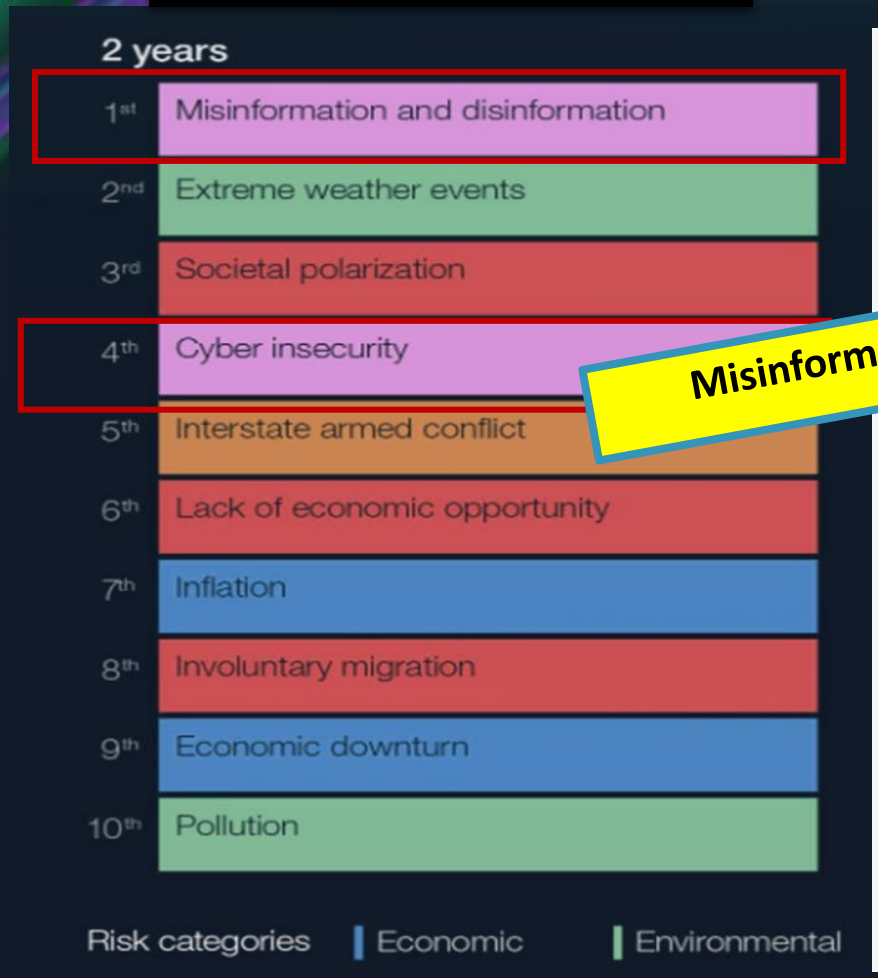
1. แนวทางการจัดการความปลอดภัยของระบบคลาวด์
2. NCSA Cloud Security Standard 2024
3. National Cloud Security Framework 2025

Download เอกสาร

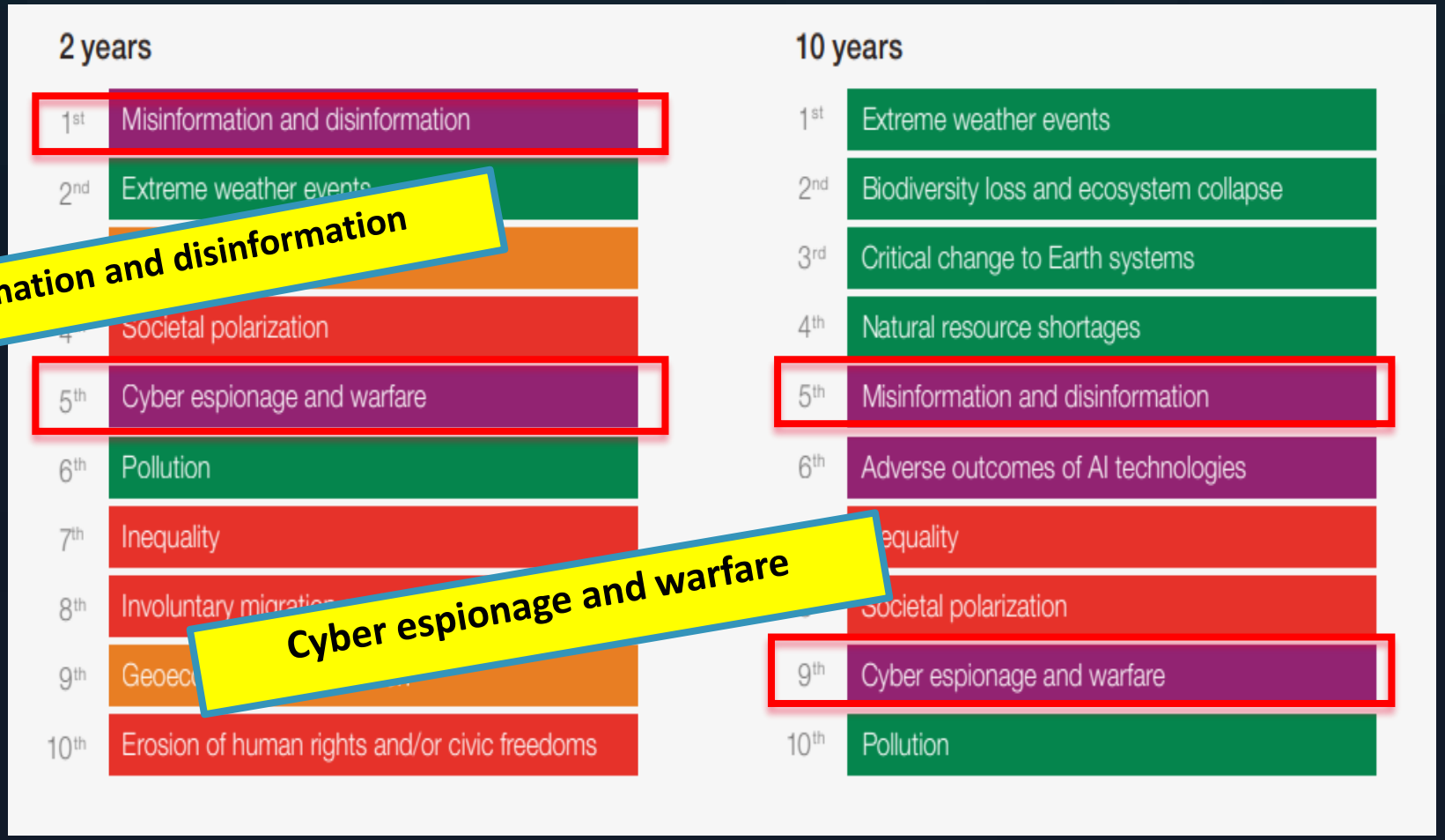
กรอบการทำงาน
cloud security

มาตรฐาน
cloud security

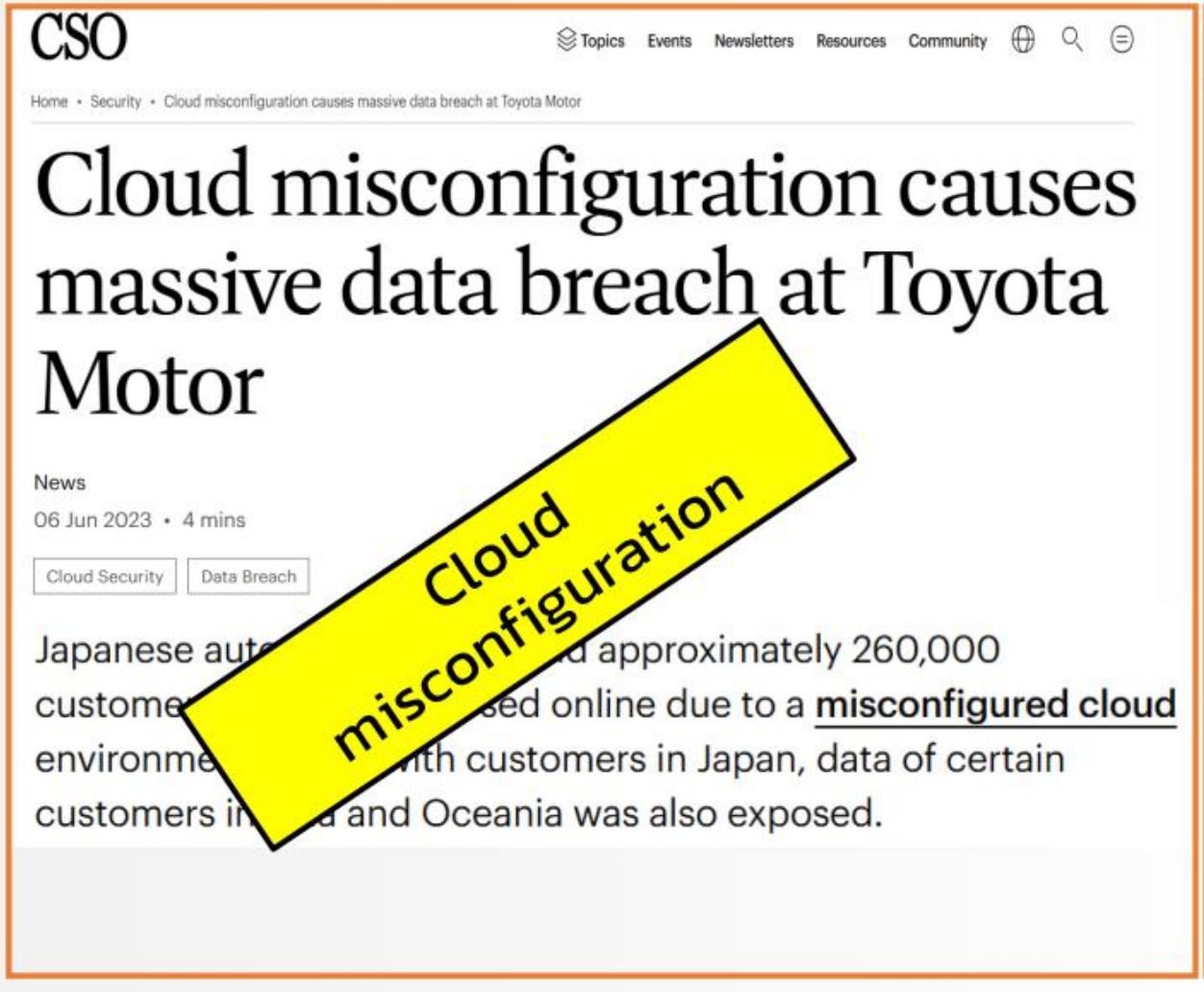
Global Risks Report 2024



Global Risks Report 2025



Data breach incidents from cloud usage



CSO

Topics Events Newsletters Resources Community

Home • Security • Cloud misconfiguration causes massive data breach at Toyota Motor

Cloud misconfiguration causes massive data breach at Toyota Motor

News

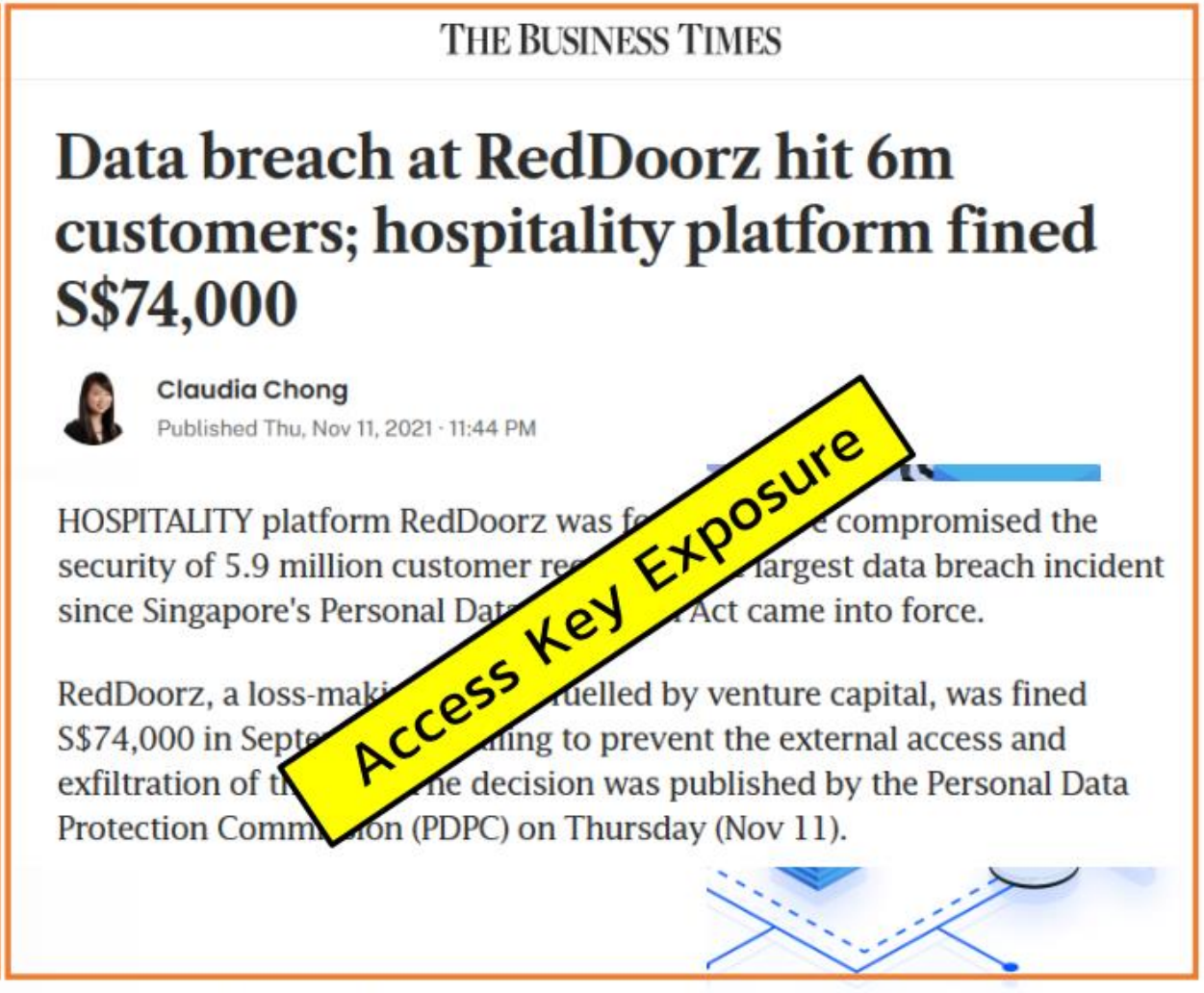
06 Jun 2023 • 4 mins

Cloud Security | Data Breach

Japanese aut… approximately 260,000 custome… sed online due to a **misconfigured cloud** environme… ith customers in Japan, data of certain customers i… and Oceania was also exposed.

Cloud misconfiguration

https://www.csoonline.com/article/575483/cloud-misconfiguration-causes-massive-data-breach-at-toyota-motor.html



THE BUSINESS TIMES

Data breach at RedDoorz hit 6m customers; hospitality platform fined S$74,000

Claudia Chong

Published Thu, Nov 11, 2021 · 11:44 PM

HOSPITALITY platform RedDoorz was f… compromised the security of 5.9 million customer re… largest data breach incident since Singapore's Personal Dat… Act came into force.

RedDoorz, a loss-maki… uelled by venture capital, was fined S$74,000 in Sept… ning to prevent the external access and exfiltration of t… he decision was published by the Personal Data Protection Comm… ion (PDPC) on Thursday (Nov 11).

Access Key Exposure

https://www.businesstimes.com.sg/startups-tech/startups/data-breach-at-reddoorz-hit-6m-customers

Major incident from cloud usage in Thailand

Bangkok Post

NEWS THAILAND BUSINESS SUSTAINABILITY LIFE GURU

BUSINESS 〉 GENERAL

Data of TrueMove H users leaked online

PUBLISHED : 15 APR 2018 AT 05:00
NEWSPAPER SECTION: NEWS WRITER: SUCHIT LEESA-NGUANSUK AND KOMSAN TORTERMVASANA

The personal data of around 46,000 TrueMove H users was leaked into Amazon Web Services' cloud storage, leading the National Broadcasting and Telecommunications Commission to call in the company for questioning. (Photo by Narupon Hinshiranan)

Summary

In April 2018, TrueMove H's e-commerce arm iTrueMart misconfigured an Amazon Web Services S3 bucket, exposing scans of customers' identity documents-including ID cards, driving licenses, and passports-without any access controls. The leak amounted to roughly 32 GB of data across approximately 46,000 files and remained publicly accessible for about a month before being secured.

Company Actions and Customer Support

TrueMove H and its partner WeMall:

- Blocked access to the exposed bucket on April 12.
- Notified potentially affected customers via SMS and email.
- Offered free identity-theft support and hot-line services.
- Emphasized that only iTrueMart customers were affected, with other customer data stored securely in internal data centers

https://www.bangkokpost.com/business/general/1446182/data-of-truemove-h-users-leaked-online
https://www.retailnews.asia/true-customers-identity-records-exposed-in-data-leak/

ตัวอย่างเคสที่เคยเกิดขึ้น

กรณี Uber
(2016)

รายละเอียด: Uber ถูกโจมตีทางไซเบอร์ที่ทำให้ข้อมูลส่วนบุคคลของผู้ใช้งานและคนขับรถกว่า 57 ล้านคนถูกเปิดเผย การโจมตีครั้งนี้เกิดขึ้นเนื่องจากข้อมูลการเข้าถึงระบบคลาวด์ของ Uber ที่ถูกเก็บไว้ใน GitHub ถูกนำมาใช้โดยผู้ไม่หวังดี

ผลกระทบ: Uber เลือกที่จะปิดบังเหตุการณ์นี้และจ่ายเงินให้กับผู้โจมตีเพื่อปิดปาก แต่เมื่อเรื่องนี้เปิดเผยออกมา Uber ถูกฟ้องร้องและเสียค่าปรับจำนวนมาก นอกจากนี้ยังส่งผลกระทบต่อชื่อเสียงของบริษัทอย่างมาก

กรณี Equifax
(2017)

รายละเอียด: Equifax ซึ่งเป็นหนึ่งในบริษัทที่ให้บริการข้อมูลเครดิตที่ใหญ่ที่สุดในโลก ประสบกับการละเมิดข้อมูลที่ร้ายแรง เนื่องจากช่องโหว่ในระบบคลาวด์ ทำให้ข้อมูลส่วนบุคคลของผู้บริโภคกว่า 147 ล้านรายถูกขโมย

ผลกระทบ: เหตุการณ์นี้ส่งผลกระทบอย่างรุนแรงต่อผู้บริโภคที่ข้อมูลส่วนบุคคลถูกเปิดเผย Equifax ต้องจ่ายค่าปรับและค่าชดเชยให้กับผู้บริโภคหลายพันล้านดอลลาร์ และต้องใช้เวลาหลายปีในการฟื้นฟูความเชื่อมั่นจากประชาชนและตลาด

กรณี Marriott International
(2018)

รายละเอียด: Marriott International ประสบกับการโจมตีทางไซเบอร์ที่เริ่มต้นในปี 2014 แต่ถูกค้นพบในปี 2018 โดยผู้โจมตีสามารถเข้าถึงข้อมูลของผู้เข้าพักกว่า 500 ล้านคนที่ถูกเก็บไว้ในระบบคลาวด์ของบริษัท

ผลกระทบ: การละเมิดครั้งนี้ทำให้ข้อมูลสำคัญของลูกค้า เช่น ชื่อ ที่อยู่ หมายเลขพาสปอร์ต และข้อมูลบัตรเครดิตถูกเปิดเผย Marriott ต้องเผชิญกับการฟ้องร้องจำนวนมากและต้องจ่ายค่าปรับที่สูงมาก

กรณี Capital One
(2019)

รายละเอียด: Capital One ประสบกับการละเมิดข้อมูลครั้งใหญ่ที่เกิดจากการกำหนดค่าคลาวด์ผิดพลาดใน Amazon Web Services (AWS) ซึ่งทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลลูกค้าได้โดยไม่ได้รับอนุญาต

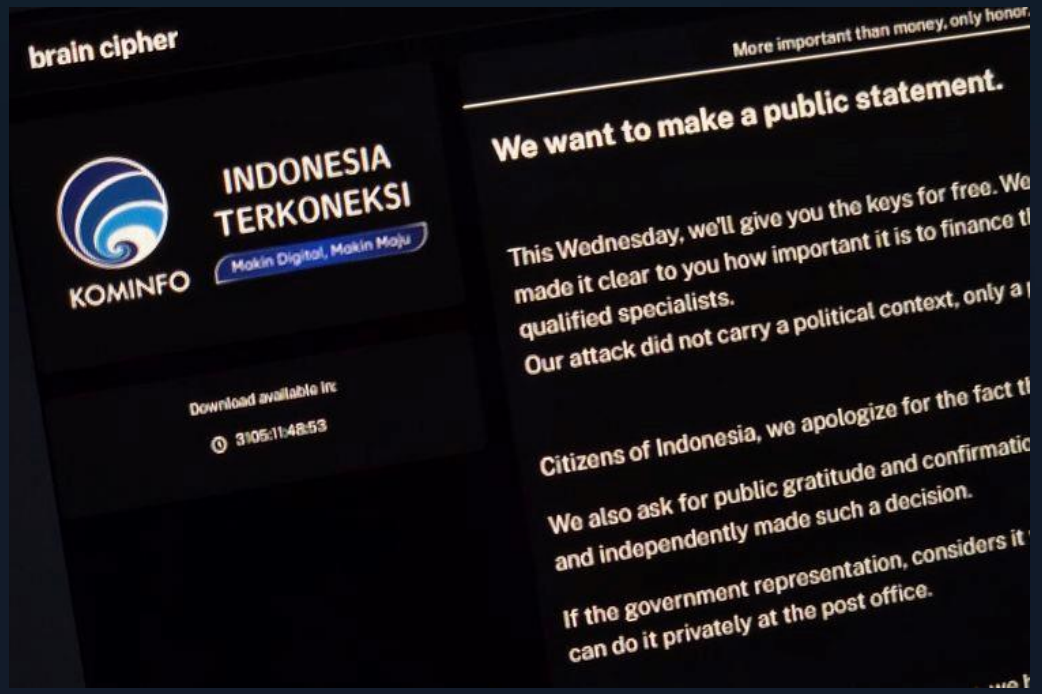
ผลกระทบ: ข้อมูลส่วนบุคคลของลูกค้ากว่า 100 ล้านรายในสหรัฐอเมริกาและ 6 ล้านรายในแคนาดาถูกเปิดเผย ทำให้ Capital One เผชิญกับการฟ้องร้องจากลูกค้าและต้องเสียเงินจำนวนมากในการแก้ไขปัญหาและปรับปรุงระบบรักษาความปลอดภัย

NCSA สกมช

ตัวอย่างเคสที่เคยเกิดขึ้น

ในปี **2021** ศูนย์ข้อมูลของรัฐบาลอินโดนีเซียถูกโจมตีทางไซเบอร์ที่ส่งผลกระทบอย่างรุนแรงต่อความปลอดภัยของข้อมูลและบริการของรัฐบาล เหตุการณ์นี้เกี่ยวข้องกับการโจมตีที่ใช้วิธีการ DDoS (Distributed Denial-of-Service)

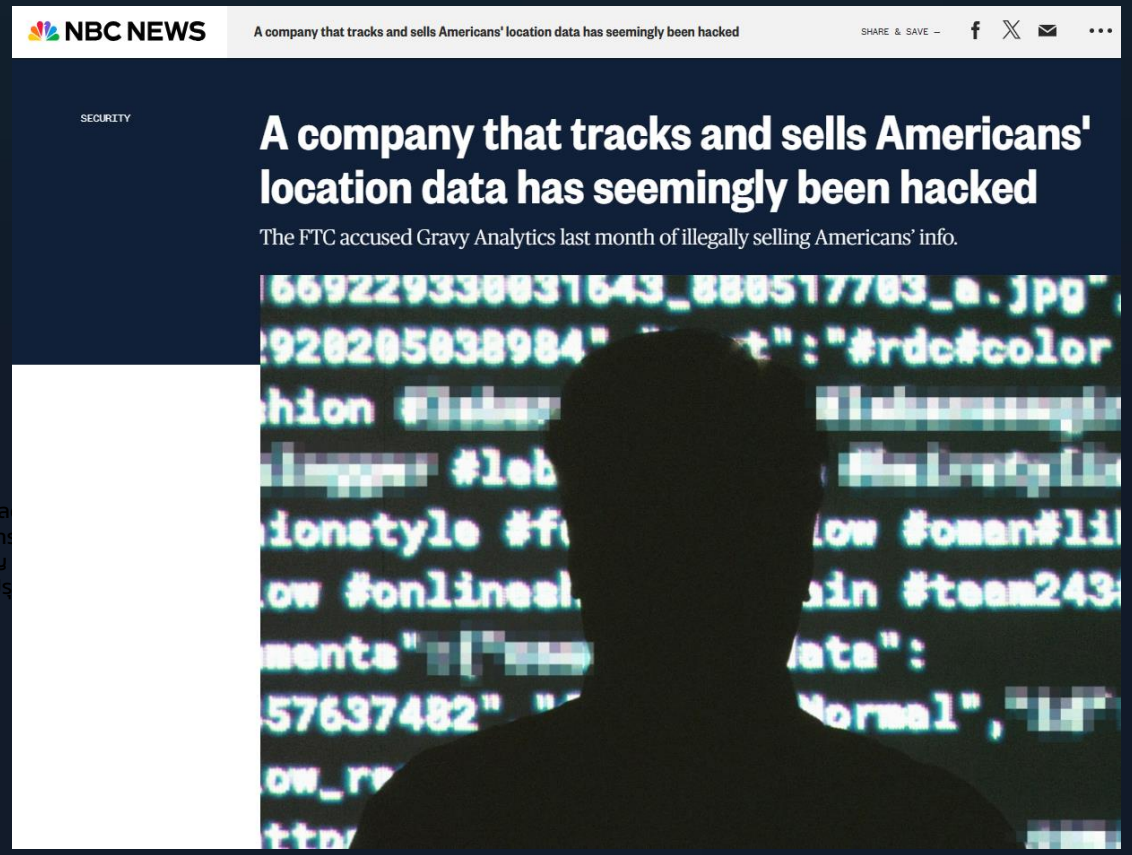
มิถุนายน **2024** ศูนย์ข้อมูลแห่งชาติของรัฐบาลอินโดนีเซีย (National Data Center หรือ PDN) ตกเป็นเหยื่อของการโจมตีทางไซเบอร์ที่รุนแรง โดยการโจมตีครั้งนี้ใช้แรนซัมแวร์ที่เรียกว่า "Brain Cipher" ซึ่งเป็นเวอร์ชันปรับปรุงของ LockBit 3.0 ที่มีความสามารถในการขโมยและเข้ารหัสข้อมูล ส่งผลให้เกิดความไม่สะดวกต่อประชาชนอย่างกว้างขวาง โดยเฉพาะที่สนามบินที่มีคิวรอนานขึ้นผู้โจมตีได้เรียกร้องค่าไถ่จำนวน ประมาณ 8 ล้านดอลลาร์สหรัฐ



ตัวอย่างเคสที่เคยเกิดขึ้น ล่าสุด ม.ค. 2025

Gravy Analytics

ในเดือนมกราคม พ.ศ. 2025 Gravy Analytics ประสบกับการละเมิดข้อมูลครั้งสำคัญซึ่งเปิดเผยข้อมูลส่วนบุคคลของผู้คนหลายล้านคนทั่วโลก แฮ็กเกอร์ใช้ประโยชน์จากข้อมูลประจำตัวที่ถูกบุกรุกเพื่อเข้าถึงที่เก็บข้อมูลบนคลาวด์ของ Gravy บนเซิร์ฟเวอร์ของ AWS



ผลกระทบ: การละเมิดอาจเกี่ยวข้องกับข้อมูลตำแหน่งของบุคคลหลายล้านคน Gravy Analytics เป็นที่ทราบกันดีว่าติดตามอุปกรณ์มากกว่าพันล้านเครื่องทั่วโลก โดยรวบรวมสัญญาณมากกว่า 17 พันล้านสัญญาณจากสมาร์ทโฟนทุกวัน

เวลาข้อมูลรั่วไหล แฮกเกอร์เอาไปโพสต์บน BF ?

MONERO

BreachForums[.]st ถูก Takedown โดย FBI

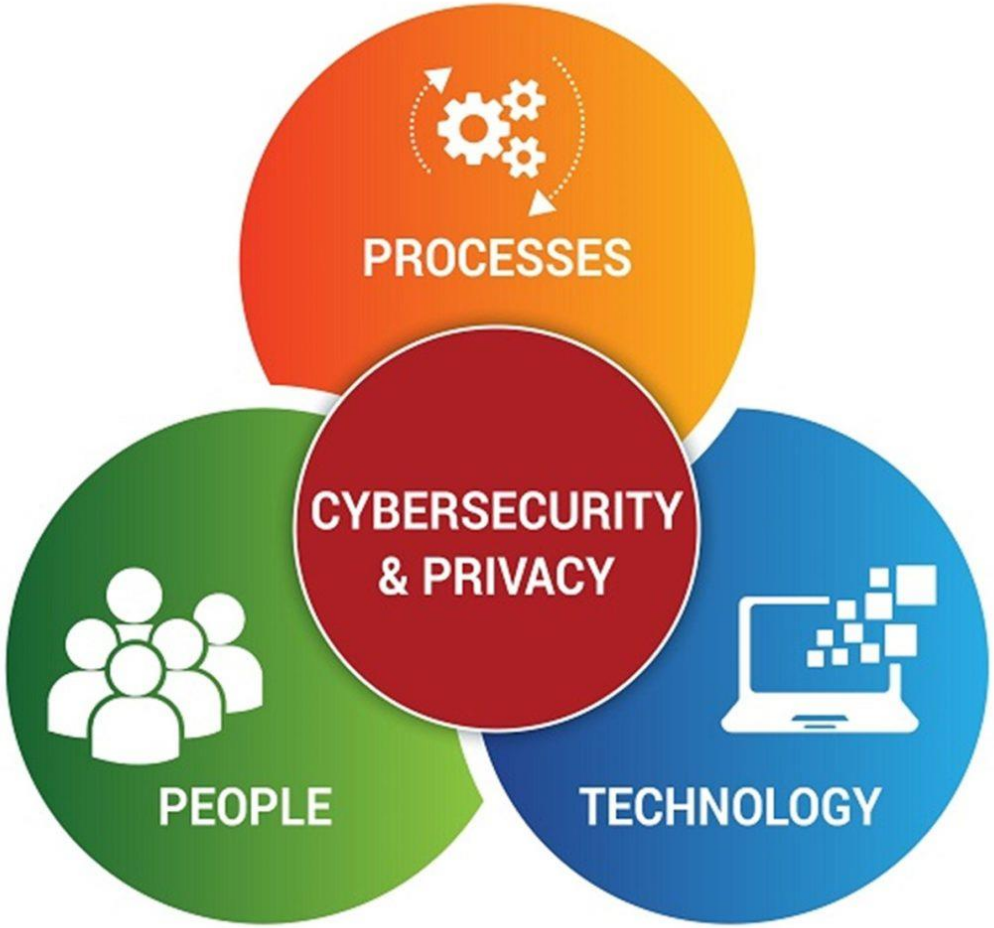
- เมื่อวันที่ 15 เมษายน พ.ศ. 2025 ZeroFox สังเกตเห็นว่า Deep Web ยอดนิยม BreachForums ไม่ได้ออนไลน์อีกต่อไป โดย BreachForums[.]st แสดงผลว่าถูก Takedown โดย FBI

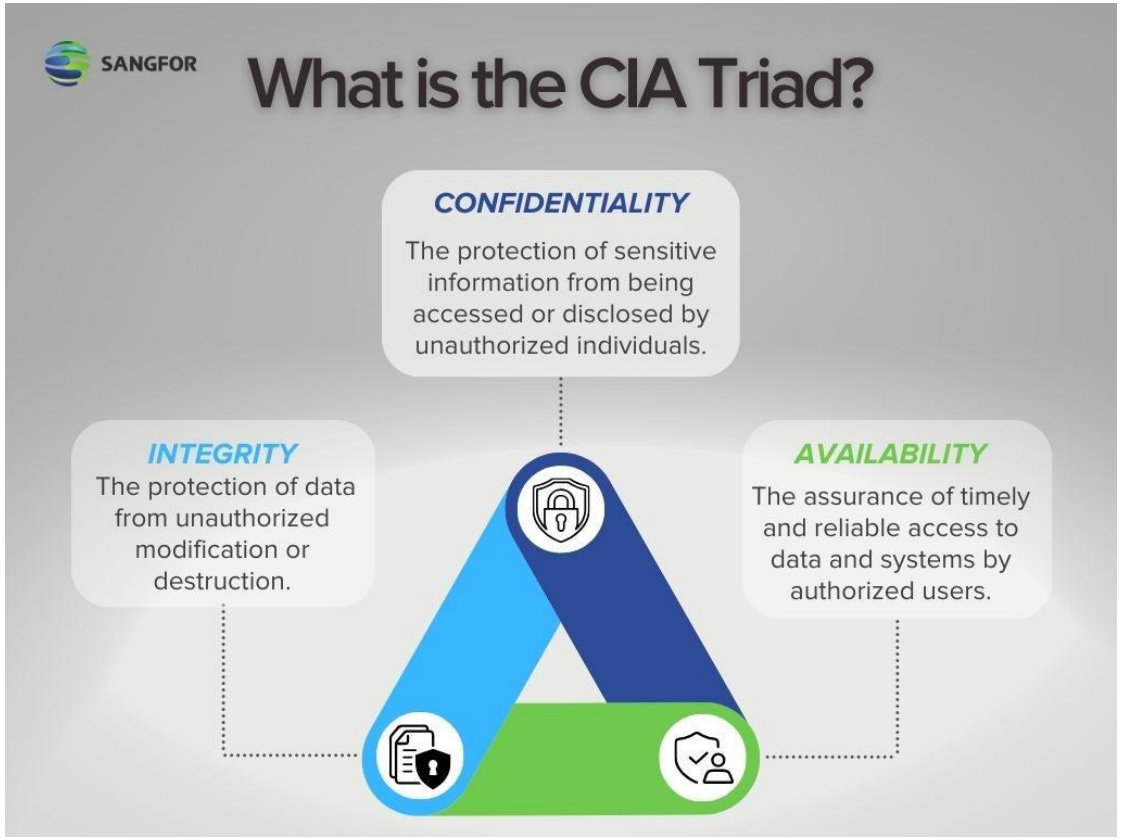
Cloud First Policy

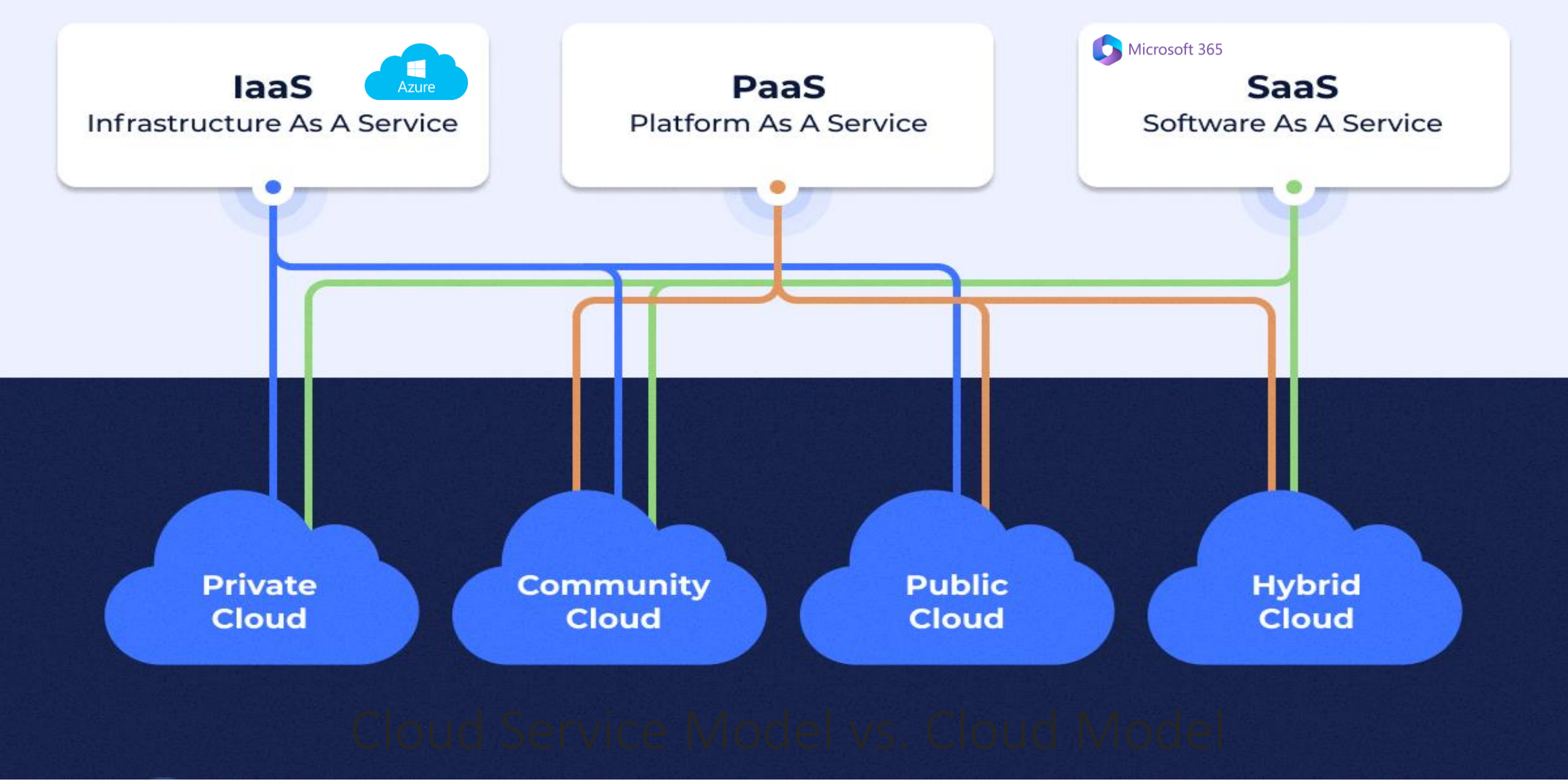
The Minister of Digital Economy and Society stated at the GOV Cloud 2023 seminar on December 16, 2023

“The capabilities of the Government Data Center Cloud service (GDCC) are being elevated to the next level. This aims to meet the increasing demands for data usage and innovation development within the public sector. **The development follows the "Cloud First Policy" concept, integrating Private Cloud and Public Cloud with standards for managing the large volume of government data.** It offers diverse software and platform services to support the public sector in creating innovative services that are easily and quickly accessible to citizens. Additionally, it includes the development of artificial intelligence (AI) innovations and promotes the safe use of AI.”

https://www.dailynews.co.th/news/2997336/


PROCESSES
CYBERSECURITY & PRIVACY
PEOPLE
TECHNOLOGY


SANGFOR
What is the CIA Triad?
CONFIDENTIALITY
The protection of sensitive information from being accessed or disclosed by unauthorized individuals.
INTEGRITY
The protection of data from unauthorized modification or destruction.
AVAILABILITY
The assurance of timely and reliable access to data and systems by authorized users.

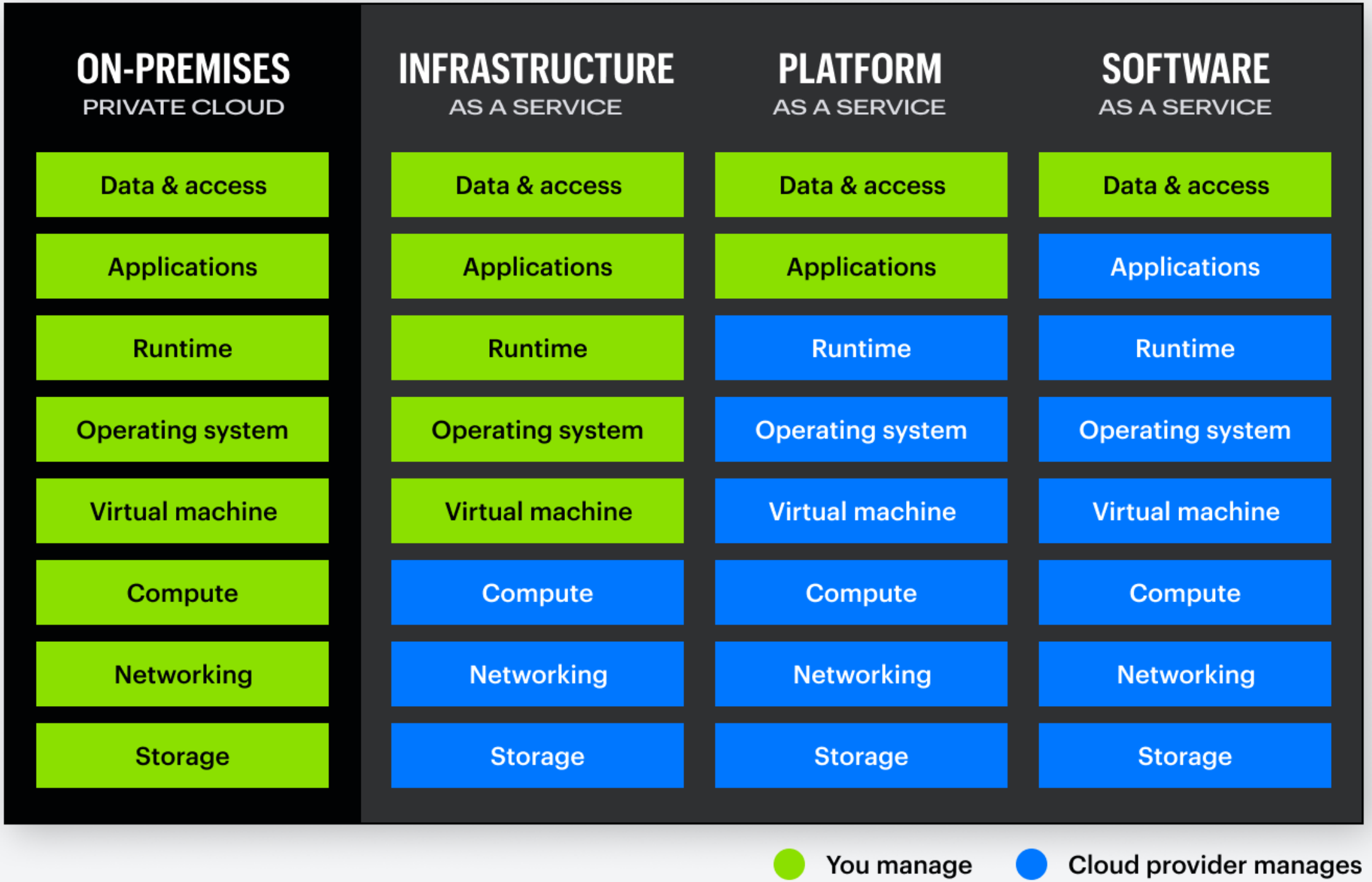


Cloud Service Model vs. Cloud Model

Shared Responsibility Model

ระหว่าง

Cloud Service Customer: CSC & Cloud Service Provider: CSP


ON-PREMISES
PRIVATE CLOUD
INFRASTRUCTURE
AS A SERVICE
PLATFORM
AS A SERVICE
SOFTWARE
AS A SERVICE
Data & access
Applications
Runtime
Operating system
Virtual machine
Compute
Networking
Storage
Data & access
Applications
Runtime
Operating system
Virtual machine
Compute
Networking
Storage
Data & access
Applications
Runtime
Operating system
Virtual machine
Compute
Networking
Storage
Data & access
Applications
Runtime
Operating system
Virtual machine
Compute
Networking
Storage
You manage
Cloud provider manages

Agenda

1. แนวทางการจัดการความปลอดภัยของระบบคลาวด์
2. NCSA Cloud Security Standard 2024
3. National Cloud Security Framework 2025

Cloud Cybersecurity Standard

แนวทางและข้อกำหนดที่ออกแบบมาเพื่อ**ปกป้องข้อมูลและบริการ**ที่อยู่**บนระบบคลาวด์**จากภัยคุกคามทางไซเบอร์มาตรฐานเหล่านี้มุ่งเน้นไปที่การจัดการความเสี่ยงความปลอดภัยในการเข้าถึงข้อมูลและการ**ป้องกันการรั่วไหลหรือการโจมตีข้อมูล** ซึ่งมักจะมีการนำมาตรฐานต่าง ๆ มาประยุกต์ใช้เพื่อให้แน่ใจว่าระบบคลาวด์มีความปลอดภัยอย่างเพียงพอ

องค์ประกอบของมาตรฐาน

หน้า ๑๖
เล่ม ๑๔๓ ตอนพิเศษ ๒๔๘ ง ราชกิจจานุเบกษา ๑๐ กันยายน ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์
พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจสร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ จึงสมควรมีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อให้การดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๙ (๔) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในคราวการประชุมครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๑๑ กรกฎาคม ๒๕๖๗ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"หน่วยงาน" หมายความว่า หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

"การประมวลผลคลาวด์" (Cloud Computing) หมายความว่า แนวคิดการเข้าถึงเครือข่ายสารสนเทศซึ่งเป็นกลุ่มทรัพยากรทางกายภาพหรือเสมือนที่สามารถแบ่งปัน (Shareable) มีความยืดหยุ่น (Elastic) และขยายขนาดได้ (Scalable) ด้วยการจัดหาตัวเอง (Self-service Provisioning) และการจัดการตามความต้องการ (Administration On-demand)

"บริการคลาวด์" (Cloud Service) หมายความว่า ความสามารถ (Capability) ในการประมวลผลคลาวด์ ซึ่งถูกเรียกใช้โดยอินเทอร์เฟซที่กำหนดไว้

"ประเภทบริการคลาวด์" (Cloud Service Category) หมายความว่า กลุ่มของบริการคลาวด์ที่มีคุณสมบัติร่วมกันบางอย่าง โดยมีรูปแบบ ดังนี้

(๑) การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service : IaaS) ประกอบด้วยระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่น ๆ ที่เกี่ยวข้องกับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ

ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 10 กันยายน 2567
**** ใช้บังคับเมื่อพ้นกำหนด 2 ปี ****

แบ่งข้อกำหนด (Requirements) ออกได้เป็น 2 ส่วน (Areas)

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์ (Cloud security governance)

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์ (Cloud infrastructure security and operation)

Ref : https://ratchakitcha.soc.go.th/documents/43184.pdf

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ด้วยนโยบายของรัฐบาลที่ต้องการขับเคลื่อนการเศรษฐกิจ การเมือง สังคม และสิ่งแวดล้อม ด้วยข้อมูลที่แม่นยำและทันสมัย เป็นรัฐบาลที่นำเอาเทคโนโลยีและระบบดิจิทัล มาใช้อย่างเต็มรูปแบบเพื่อประโยชน์ของประเทศชาติและประชาชน มุ่งเน้นการบริหารประเทศในรูปแบบบูรณาการการทำงานร่วมกันระหว่างหน่วยงาน

นโยบาย Cloud First Policy จึงเป็นหนึ่งในการริเริ่มที่เป็นรูปธรรมที่ตอบสนองต่อนโยบายรัฐบาล โดยการกำหนดให้หน่วยงานของรัฐ มีการใช้ประโยชน์จากคลาวด์ อย่างจริงจังมุ่งเน้นการลดค่าใช้จ่ายของภาครัฐที่ต้องจัดซื้อระบบคอมพิวเตอร์แม่ข่ายเป็นของหน่วยงานเอง ซึ่งมีภาระด้านการบำรุงรักษา อีกทั้งเป็นจุดเริ่มต้นที่สำคัญของการบูรณาการข้อมูลระหว่างกัน

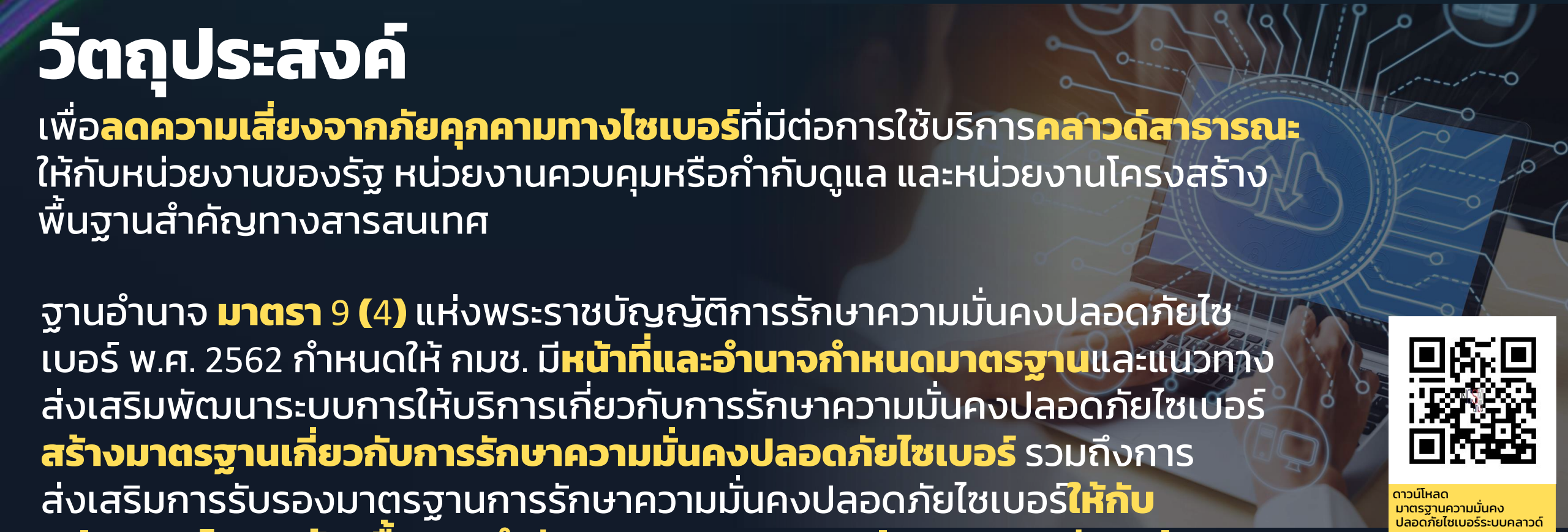
สกมช. ในฐานะหน่วยงานระดับชาติที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ จึงได้จัดทำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อสนับสนุนต่อนโยบาย Cloud First Policy และเพื่อให้หน่วยงานของรัฐรวมทั้งภาคเอกชนที่เกี่ยวข้อง ได้รับประโยชน์สูงสุดจากการดำเนินการตามนโยบายดังกล่าว

ให้มีผลใช้บังคับ เมื่อพ้นกำหนดสองปี นับแต่วันที่ประกาศในราชกิจจานุเบกษา เป็นต้นไป (10 ก.ย. 2569)

NCSA สกมช

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567



วัตถุประสงค์

เพื่อ**ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์**ที่มีต่อการใช้บริการ**คลาวด์สาธารณะ**ให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

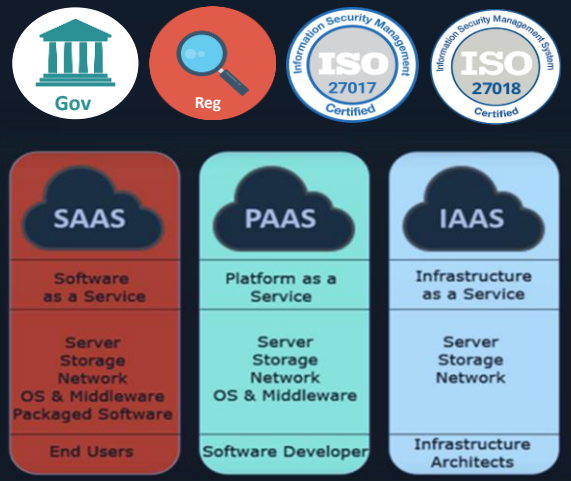
ฐานอำนาจ **มาตรา** 9 **(**4**)** แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้ กมช. มี**หน้าที่และอำนาจกำหนดมาตรฐาน**และแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ **สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์** รวมถึงการส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์**ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน**

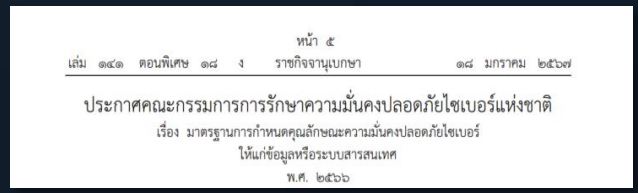
ดาวน์โหลด
มาตรฐานความมั่นคง
ปลอดภัยไซเบอร์ระบบคลาวด์
พ.ศ. 2567

NCSA สกมช

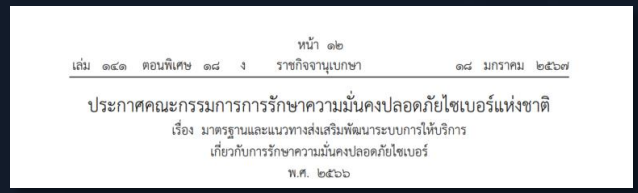
ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

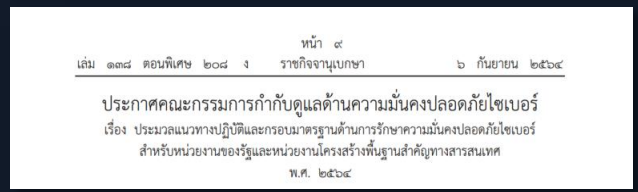



หน้า ๕
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์
ให้แก่ข้อมูลหรือระบบสารสนเทศ
พ.ศ. ๒๕๖๖


หน้า ๑๒
เล่ม ๑๔๑ ตอนพิเศษ ๑๘ ง ราชกิจจานุเบกษา ๑๘ มกราคม ๒๕๖๗

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ
เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๖


หน้า ๙
เล่ม ๑๓๘ ตอนพิเศษ ๒๐๘ ง ราชกิจจานุเบกษา ๖ กันยายน ๒๕๖๔

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
พ.ศ. ๒๕๖๔

NCSA สกมช

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์

2.2 การจัดการทรัพย์สิน

2.3 การควบคุมการเข้าถึง

2.4 การเข้ารหัส

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม

2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย

2.8 การจัดหา การพัฒนา และการบำรุงรักษา

2.9 การจัดการผู้ให้บริการภายนอก

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

ขั้นกำหนดขั้นต่ำ

ผลกระทบระดับต่ำ

- ทำตามข้อกำหนดข้อ : 5.1.1 5.1.2 5.2.1 5.2.2 5.2.3 5.2.4 5.2.8 5.2.9
- การตรวจรับรองสำหรับ**ผู้ใช้บริการ** : **ประเมินตนเอง** อย่างน้อยปีละ 1 ครั้ง
- การตรวจรับรองสำหรับ**ผู้ให้บริการ** : ได้รับการตรวจรับรองโดย**หน่วยงานให้บริการตรวจรับรอง** ตามวงรอบ 3 ปี (ปีที่ 1 ตรวจรับรอง -> ปีที่ 2-3 ตรวจสำรวจ) **และได้รับการรับรองมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite** เป็นอย่างน้อย

ผลกระทบระดับกลาง

- **ทำตามข้อกำหนดข้อ :** 5.1.1 5.1.2 5.1.3 5.2.1 5.2.2 5.2.3 5.2.4 5.2.7 5.2.8 5.2.9 5.2.10
- **การตรวจรับรองสำหรับผู้ใช้บริการ :** โดย Reg หรือ หน่วยงานที่ได้รับการรับรอง โดย**หน่วยงานให้บริการตรวจรับรอง** (Certify Body) ตามวงรอบ 3 ปี (ปีที่ 1 ตรวจรับรอง -> ปีที่ 2-3 ตรวจสำรวจ)
- **การตรวจรับรองสำหรับผู้ให้บริการ :** โดย**หน่วยงานให้บริการตรวจรับรอง** (Certify Body) ตามวงรอบ 3 ปี และ**ได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification** เป็นอย่างน้อย

ผลกระทบระดับสูง

- **ทำตามข้อกำหนดข้อ : ทุกข้อ**
- **การตรวจรับรองสำหรับผู้ใช้บริการ : โดยหน่วยงานให้บริการตรวจรับรอง**
- **การตรวจรับรองสำหรับผู้ให้บริการ : โดยหน่วยงานให้บริการตรวจรับรอง และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย**

NCSA สกมช

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

กระบวนการตรวจ รับรองมาตรฐาน

ผลกระทบระดับต่ำ

- ทำตามข้อกำหนดข้อ : 5.1.1 5.1.2 5.2.1 5.2.2 5.2.3 5.2.4 5.2.8 5.2.9
- การตรวจรับรองสำหรับ**ผู้ใช้บริการ** **ประเมินตนเอง** อย่างน้อยปีละ 1 ครั้ง
- การตรวจรับรองสำหรับ**ผู้ให้บริการ** : ได้รับการตรวจรับรองโดย**หน่วยงานให้บริการตรวจรับรอง** ตามวงรอบ 3 ปี (ปีที่ 1 ตรวจรับรอง -> ปีที่ 2–3 ตรวจสำรวจ)

และ ได้รับการรับรองมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย

การประเมินตนเอง (Self-assessment) เป็นการประเมินหน่วยงานของตนตามรูปแบบที่สำนักงานกำหนด พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย

การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่า ตามประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

และ ISO 27001 และ STAR LEVEL ONE Lite CCM

ดาวน์โหลด มาตรฐานความมั่นคงปลอดภัยไซเบอร์ ระบบคลาวด์ พ.ศ. 2567

NCSA สกมช

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

กระบวนการตรวจ รับรองมาตรฐาน

การตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) เป็นการตรวจรับรองโดยหน่วยงานควบคุมหรือกำกับดูแลตามประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล

หรือ

การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่าตามประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่า ตามประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

และ STAR LEVEL TWO: THIRD-PARTY AUDIT — SECURITY TRUST ASSURANCE & RISK — CCM Cloud Controls Matrix **และ** ISO ISO 27701

ผลกระทบระดับกลาง

- ทำตามข้อกำหนดข้อ : 5.1.1 5.1.2 5.1.3 5.2.1 5.2.2 5.2.3 5.2.4 5.2.7 5.2.8 5.2.9 5.2.10
- การตรวจรับรองสำหรับ**ผู้ใช้บริการ** : โดยหน่วยงานควบคุมหรือกำกับดูแล หรือโดยหน่วยงานที่ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ 3 ปี (ปีที่ 1 ตรวจรับรอง -> ปีที่ 2-3 ตรวจสำรวจ)
- การตรวจรับรองสำหรับ**ผู้ให้บริการ** : โดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ 3 ปี และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

*In order for you to be eligible for CSA STAR Level 2 Certification, you must have or obtain an ISO/IEC 27001 certification from an accredited certification body.

**STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM).

NCSA สกมช

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567

กระบวนการตรวจรับรองมาตรฐาน

ผลกระทบระดับสูง

**STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM).

การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่า ตามประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

การตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) เป็นการตรวจรับรองโดยหน่วยงานให้บริการตรวจรับรองในระดับขั้นก้าวหน้าหรือสูงกว่า ตามประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

และ ISO 27017 Certified หรือ STAR LEVEL TWO และ CCM และ ISO 27018 Certified และ ISO 27701

- ทำตามข้อกำหนดข้อ : ทุกข้อ
- การตรวจรับรองสำหรับผู้ใช้บริการ : โดยหน่วยงานให้บริการตรวจรับรอง ตามวงรอบ 3 ปี
- การตรวจรับรองสำหรับผู้ให้บริการ : โดยหน่วยงานให้บริการตรวจรับรอง ตามวงรอบ 3 ปี และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2 /CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

*In order for you to be eligible for CSA STAR Level 2 Certification, you must have or obtain an ISO/IEC 27001 certificate from an accredited certification body.

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์ 5.2.1

2.2 การจัดการทรัพย์สิน 5.2.2

2.3 การควบคุมการเข้าถึง 5.2.3

2.4 การเข้ารหัส 5.2.4

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5

2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7

2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8

2.9 การจัดการผู้ให้บริการภายนอก 5.2.9

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับการประมวลผลบนคลาวด์	ต้องเพิ่มนโนบายการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อจัดการกับการจัดหา และใช้บริการคลาวด์
นโยบายคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการคลาวด์ ต้องระบุข้อความเกี่ยวกับข้อตกลงทางสัญญาระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลบนคลาวด์ กับผู้ใช้บริการคลาวด์	

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องตกลงกับผู้ให้บริการคลาวด์เกี่ยวกับบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม และผู้ใช้บริการคลาวด์ต้องยืนยันว่าสามารถทำหน้าที่และความรับผิดชอบที่ทั้งสองฝ่ายตกลงกันไว้ได้	ต้องตกลงและแบ่งบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมกับผู้ใช้บริการคลาวด์ และผู้ให้บริการภายนอก
ต้องระบุและจัดการส่วนงานที่มีหน้าที่สัมพันธ์กับผู้ให้บริการคลาวด์	ต้องแต่งตั้งผู้ประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องพิจารณากฎหมายและข้อบังคับที่ควบคุมผู้ให้บริการคลาวด์	ต้องแจ้งผู้ใช้บริการคลาวด์ทราบถึงเขตอำนาจศาลที่ควบคุมผู้ให้บริการคลาวด์
ต้องขอหลักฐานที่ว่าผู้ให้บริการคลาวด์ได้ปฏิบัติตามกฎระเบียบและมาตรฐานที่เกี่ยวข้องกับผู้ใช้บริการคลาวด์	ต้องระบุข้อกำหนดทางกฎหมายที่เกี่ยวข้องกับตนเองและแจ้งผู้ใช้บริการคลาวด์ทราบเมื่อได้รับการร้องขอ
ต้องระบุข้อกำหนดในการให้สิทธิใช้งานซอฟต์แวร์เฉพาะระบบคลาวด์ที่ติดตั้งซอฟต์แวร์	ต้องกำหนดกระบวนการในการตอบสนองการร้องเรียนเรื่องสิทธิในทรัพย์สินทางปัญญา
ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับปกป้องบันทึกการเข้าใช้งาน ที่รวบรวมและจัดเก็บโดยผู้ให้บริการคลาวด์	ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการปกป้องบันทึกการเข้าใช้งานของผู้ใช้บริการคลาวด์
ต้องตรวจสอบชุดมาตรการควบคุมการเข้ารหัสข้อมูลว่าสอดคล้องกับกฎหมาย	ต้องอธิบายผู้ใช้บริการคลาวด์เกี่ยวกับมาตรการควบคุมการเข้ารหัสข้อมูล

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องสร้างความตระหนักรู้ การศึกษา การฝึกอบรม ผู้จัดการบริการบนคลาวด์ ผู้ดูแลระบบบริการคลาวด์ ผู้ใช้บริการคลาวด์ พนักงาน	ต้องสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและด้านการคุ้มครองข้อมูลส่วนบุคคล แก่พนักงาน

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์ 5.2.1

2.2 การจัดการทรัพย์สิน 5.2.2

2.3 การควบคุมการเข้าถึง 5.2.3

2.4 การเข้ารหัส 5.2.4

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5

2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7

2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8

2.9 การจัดการผู้ให้บริการภายนอก 5.2.9

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ทะเบียนทรัพย์สินต้องคำนึงถึงข้อมูลและทรัพย์สินซึ่งจัดเก็บในสภาพแวดล้อมการประมวลผลบนคลาวด์	ทะเบียนทรัพย์สินของผู้ให้บริการคลาวด์ต้องระบุอย่างชัดเจนในเรื่อง ข้อมูลผู้ใช้บริการคลาวด์ ข้อมูลที่เกิดจากการใช้บริการคลาวด์
ต้องบ่งชี้ (Labelling) ข้อมูลและทรัพย์สินที่ใช้งานหรือเก็บรักษาบนคลาวด์	ต้องจัดทำเอกสารและเปิดเผยฟังก์ชันการทำงานของบริการที่ผู้ใช้บริการสามารถนำไปใช้เพื่อการบ่งชี้ (Labeling) ข้อมูลและทรัพย์สินที่เกี่ยวข้อง

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องระบุข้อกำหนดสำหรับการเข้าถึงบริการคลาวด์	
การลงทะเบียนและยกเลิกการลงทะเบียนผู้ใช้ ต้องครอบคลุมสถานการณ์ที่การเข้าถึงของผู้ใช้ถูกละเมิด	ต้องเตรียมฟังก์ชันการลงทะเบียนและการยกเลิกการลงทะเบียนผู้ใช้งาน
ต้องใช้เทคนิคการยืนยันตัวตนที่เพียงพอสำหรับผู้ดูแลระบบ	ต้องมีเทคนิคการยืนยันตัวตนที่เพียงพอสำหรับผู้ดูแลระบบของผู้ใช้บริการคลาวด์
ต้องสามารถจัดการเข้าถึงข้อมูลได้ตามนโยบายการควบคุมการเข้าถึง	ต้องให้บริการการควบคุมการเข้าถึงแก่ผู้ใช้บริการคลาวด์
หากอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ ต้องระบุโปรแกรมที่จะใช้ และตรวจสอบว่าโปรแกรมเหล่านั้นไม่รบกวนการบริการคลาวด์	ต้องระบุข้อกำหนดสำหรับโปรแกรมอรรถประโยชน์ ที่ใช้ในบริการคลาวด์
ต้องปฏิบัติตามการเข้าสู่ระบบอย่างปลอดภัย	ต้องให้มีขั้นตอนการเข้าสู่ระบบอย่างปลอดภัยแก่ผู้ใช้บริการ

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องใช้มาตรการควบคุมการเข้ารหัสที่แข็งแรง	ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเข้ารหัส
ต้องระบุกุญแจสำหรับการเข้ารหัส	
ถ้ามีฟังก์ชันการจัดการกุญแจต้องมีข้อกำหนดเฉพาะสำหรับการบริหารจัดการ	
ต้องไม่อนุญาตให้ผู้ให้บริการคลาวด์จัดเก็บและจัดการกุญแจ	

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

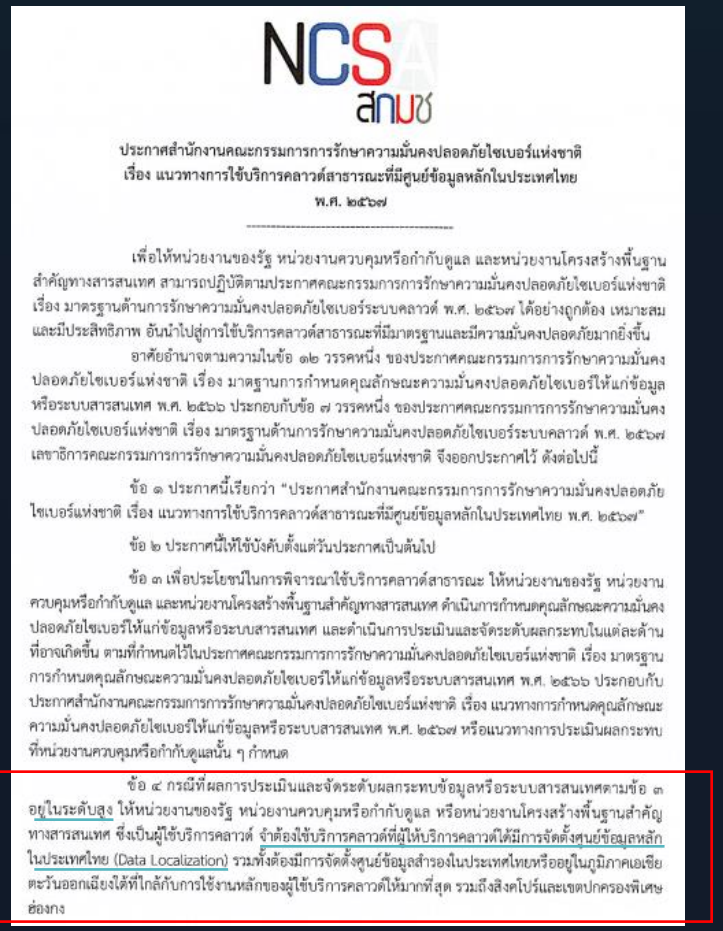
ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องใช้ศูนย์ข้อมูลหลักในประเทศไทย	ต้องตั้งศูนย์ข้อมูลหลักในประเทศไทย
	ต้องตั้งศูนย์ข้อมูลสำรองในประเทศไทย หรือในภูมิภาคเอเชียตะวันออกเฉียงใต้ รวมถึงสิงคโปร์และฮ่องกง
ต้องให้ผู้ให้บริการคลาวด์ยืนยันว่ามีนโยบายและขั้นตอนการกำจัด หรือนำทรัพยากรกลับมาใช้ใหม่	ต้องตรวจสอบว่ามีการเตรียมการสำหรับการกำจัด หรือนำทรัพยากรกลับมาใช้ใหม่อย่างปลอดภัย

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

ประกาศ กมช. เรื่องแนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. ๒๕๖๗

ดาวน์โหลด
ประกาศฯ ศูนย์ข้อมูลหลักในประเทศไทย
พ.ศ. 2567



NCS สกมช

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย
พ.ศ. ๒๕๖๗

เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ได้อย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ อันนำไปสู่การใช้บริการคลาวด์สาธารณะที่มีมาตรฐานและมีความมั่นคงปลอดภัยมากยิ่งขึ้น

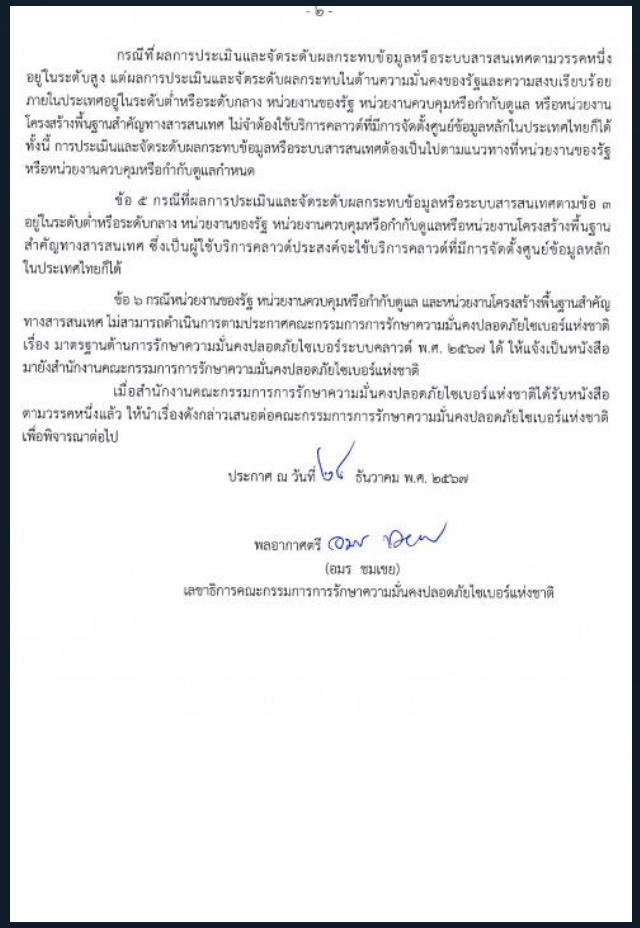
อาศัยอำนาจตามความในข้อ ๑๒ วรรคหนึ่ง ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ ประกอบกับข้อ ๗ วรรคหนึ่ง ของประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการใช้บริการคลาวด์สาธารณะที่มีศูนย์ข้อมูลหลักในประเทศไทย พ.ศ. ๒๕๖๗"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ เพื่อประโยชน์ในการพิจารณาใช้บริการคลาวด์สาธารณะ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ และดำเนินการประเมินและจัดระดับผลกระทบในแต่ละด้านที่อาจเกิดขึ้น ตามที่กำหนดไว้ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ ประกอบกับประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๗ หรือแนวทางการประเมินผลกระทบที่หน่วยงานควบคุมหรือกำกับดูแลนั้น ๆ กำหนด

ข้อ ๔ กรณีที่ผลการประเมินและจัดระดับผลกระทบข้อมูลหรือระบบสารสนเทศตามข้อ ๓ อยู่ในระดับสูง ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นผู้ใช้บริการคลาวด์ จำต้องใช้บริการคลาวด์ที่ผู้ให้บริการคลาวด์ได้มีการจัดตั้งศูนย์ข้อมูลหลักในประเทศไทย (Data Localization) รวมทั้งต้องมีการจัดตั้งศูนย์ข้อมูลสำรองในประเทศไทยหรืออยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ใกล้กับการใช้งานหลักของผู้ใช้บริการคลาวด์ให้มากที่สุด รวมถึงสิงคโปร์และเขตปกครองพิเศษฮ่องกง



- ๒ -

กรณีที่ผลการประเมินและจัดระดับผลกระทบข้อมูลหรือระบบสารสนเทศตามวรรคหนึ่งอยู่ในระดับสูง แต่ผลการประเมินและจัดระดับผลกระทบในด้านความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศอยู่ในระดับต่ำหรือระดับกลาง หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่จำต้องใช้บริการคลาวด์ที่มีการจัดตั้งศูนย์ข้อมูลหลักในประเทศไทยก็ได้ ทั้งนี้ การประเมินและจัดระดับผลกระทบข้อมูลหรือระบบสารสนเทศต้องเป็นไปตามแนวทางที่หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแลกำหนด

ข้อ ๕ กรณีที่ผลการประเมินและจัดระดับผลกระทบข้อมูลหรือระบบสารสนเทศตามข้อ ๓ อยู่ในระดับต่ำหรือระดับกลาง หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นผู้ใช้บริการคลาวด์ประสงค์จะใช้บริการคลาวด์ที่มีการจัดตั้งศูนย์ข้อมูลหลักในประเทศไทยก็ได้

ข้อ ๖ กรณีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่สามารถดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ได้ ให้แจ้งเป็นหนังสือมายังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เมื่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้รับหนังสือตามวรรคหนึ่งแล้ว ให้นำเรื่องดังกล่าวเสนอต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อพิจารณาต่อไป

ประกาศ ณ วันที่ ๒๔ ธันวาคม พ.ศ. ๒๕๖๗

พลอากาศตรี (อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องคำนึงถึงผลกระทบของการเปลี่ยนแปลงใด ๆ ทีเกิดจากผู้ให้บริการคลาวด์	ต้องให้ข้อมูลแก่ผู้ใช้บริการคลาวด์เกี่ยวกับการเปลี่ยนแปลงในบริการคลาวด์ที่อาจส่งผลเสียต่อบริการ รวมถึงความมั่นคงปลอดภัยสารสนเทศ และต้องแจ้งผู้ใช้บริการคลาวด์ทราบ
ต้องตรวจสอบว่าความสามารถของทรัพยากรคลาวด์เป็นไปตามข้อกำหนด	ต้องตรวจสอบขีดความสามารถของทรัพยากรเพื่อป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการขาดแคลนทรัพยากร
ต้องขอข้อมูลของความสามารถในการสำรองข้อมูลจากผู้ให้บริการคลาวด์	ต้องให้ข้อมูลของความสามารถในการสำรองข้อมูลแก่ผู้ใช้บริการคลาวด์
ต้องมีการบันทึกเหตุการณ์ (Event Logging)	ต้องให้ผู้ใช้บริการคลาวด์สามารถบันทึกเหตุการณ์
ต้องขอข้อมูลการจัดการช่องโหว่	ต้องให้ข้อมูลการจัดการช่องโหว่

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องมีการระบบบันทึกที่มีการนำข้อมูลส่วนบุคคลผ่านเข้าออก รวมถึงสื่อทางกายภาพที่ใช้ด้วย	
ต้องขอให้ผู้ให้บริการคลาวด์ใช้มาตรการเพิ่มเติม เช่น เข้ารหัส เพื่อให้มั่นใจว่าข้อมูลมีความปลอดภัยตั้งแต่ต้นทาง-ปลายทาง	หากเป็นไปได้ ต้องขอให้ผู้ใช้บริการคลาวด์ใช้มาตรการเพื่อให้มั่นใจว่าข้อมูลมีความปลอดภัยตั้งแต่ต้นทาง - ปลายทาง
ต้องมีการแยกเครือข่ายเพื่อให้แยกผู้เช่า	ต้องบังคับใช้การแยกการเข้าถึงเครือข่ายในกรณีมีผู้เช่าหลายราย

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

- 1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1
- 1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2
- 1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

- 2.1 การบริหารทรัพยากรมนุษย์ 5.2.1
- 2.2 การจัดการทรัพย์สิน 5.2.2
- 2.3 การควบคุมการเข้าถึง 5.2.3
- 2.4 การเข้ารหัส 5.2.4
- 2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5
- 2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6
- 2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7
- 2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8
- 2.9 การจัดการผู้ให้บริการภายนอก 5.2.9
- 2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ และประเมินบริการของผู้ให้บริกาคลาวด์ว่าตอบสนองความต้องการ	ต้องให้ข้อมูลเกี่ยวกับความสามารถในการรักษาความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้บริการคลาวด์
ต้องขอข้อมูลจากผู้ให้บริการคลาวด์เกี่ยวกับการพัฒนาบริการ (เช่น SaaS) อย่างปลอดภัย	ต้องให้ข้อมูลเกี่ยวกับการพัฒนาความปลอดภัย โดยสอดคล้องกับนโยบายการเปิดเผยข้อมูล

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์ 5.2.1

2.2 การจัดการทรัพย์สิน 5.2.2

2.3 การควบคุมการเข้าถึง 5.2.3

2.4 การเข้ารหัส 5.2.4

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5

2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7

2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8

2.9 การจัดการผู้ให้บริการภายนอก 5.2.9

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องระบุว่าผู้ให้บริการคลาวด์เป็นผู้ให้บริการภายนอกประเภทหนึ่ง ซึ่งจะช่วยลดความเสี่ยงเกี่ยวกับการเข้าถึงและการจัดการข้อมูล	
ต้องยืนยันบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การป้องกันมัลแวร์ การสำรองข้อมูล การจัดการช่องโหว่	ต้องระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องซึ่งใช้เป็นส่วนหนึ่งของข้อตกลงเพื่อไม่ให้เกิดการเข้าใจผิดระหว่างผู้ให้บริการและผู้ใช้บริการคลาวด์
	หากใช้บริการจากผู้ให้บริการรายย่อย ต้องตรวจสอบระดับความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการรายย่อยนั้น

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

โครงสร้างของมาตรฐาน

1. การกำกับดูแลด้านความมั่นคงปลอดภัยระบบคลาวด์

1.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.1

1.2 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยสารสนเทศ 5.1.2

1.3 การปฏิบัติตามกฎ ระเบียบ ข้อบังคับ 5.1.3

2. การปฏิบัติการและการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานระบบคลาวด์

2.1 การบริหารทรัพยากรมนุษย์ 5.2.1

2.2 การจัดการทรัพย์สิน 5.2.2

2.3 การควบคุมการเข้าถึง 5.2.3

2.4 การเข้ารหัส 5.2.4

2.5 การรักษาความปลอดภัยทางกายภาพและสภาพแวดล้อม 5.2.5

2.6 การรักษาความมั่นคงปลอดภัยการปฏิบัติการ 5.2.6

2.7 การรักษาความมั่นคงปลอดภัยเครือข่าย 5.2.7

2.8 การจัดหา การพัฒนา และการบำรุงรักษา 5.2.8

2.9 การจัดการผู้ให้บริการภายนอก 5.2.9

2.10 การจัดการเหตุภัยคุกคามทางสารสนเทศ 5.2.10

ผู้ใช้บริการคลาวด์	ผู้ให้บริการคลาวด์
ต้องตรวจสอบการจัดความรับผิดชอบสำหรับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	ต้องกำหนดขอบเขตความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ
ภัยคุกคามทางสารสนเทศต้องนำไปสู่การทบทวนโดยผู้ใช้บริการคลาวด์ หรือทบทวนร่วมกันกับผู้ให้บริการคลาวด์	ต้องเตรียมเอกสารที่เกี่ยวข้องให้กับผู้ใช้บริการคลาวด์
ต้องขอข้อมูลเกี่ยวกับ การรายงานเหตุการณ์ความมั่นคงปลอดภัย และติดตามสถานะของเหตุการณ์นั้น	ต้องมีกลไกสำหรับรายงานเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการติดตามสถานะฯ

Legend: 5.2.5 ตรงกับหัวข้อในมาตรฐานคลาวด์

NCSA สกมช

ข้อกำหนดขั้นต่ำ

ประเภทของข้อมูลหรือระบบสารสนเทศ*	ข้อกำหนดขั้นต่ำ	การตรวจรับรองสำหรับผู้ใช้บริการคลาวด์	การตรวจรับรองสำหรับผู้ให้บริการคลาวด์
ผลกระทบระดับต่ำ **ต่ำ**	ข้อกำหนดส่วนที่ ๑ - เฉพาะข้อ ๕.๑.๑, ๕.๑.๒ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๘, ๕.๒.๙	ประเมินตนเอง (Self-assessment) พร้อมแนบหลักฐานและขออนุมัติไปยังผู้บริหารสูงสุดของหน่วยงาน โดยเก็บรักษาไว้ที่หน่วยงานและส่งให้สำนักงานด้วย	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 Certification และ CSA STAR Level 1/CCM Lite เป็นอย่างน้อย
ผลกระทบระดับกลาง **กลาง**	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - เฉพาะข้อ ๕.๒.๑, ๕.๒.๒, ๕.๒.๓, ๕.๒.๔, ๕.๒.๗, ๕.๒.๘, ๕.๒.๙, ๕.๒.๑๐	ได้รับการรับรองโดยหน่วยงานควบคุมหรือกำกับดูแล (Attestation) หรือ ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน CSA STAR Level 2/CCM และ ISO/IEC 27701 Certification เป็นอย่างน้อย

ระดับผลกระทบ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้องครบถ้วน (Integrity)	สภาพพร้อมใช้งาน (Availability)
ระดับต่ำ	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับ**	**การแก้ไขหรือทำลายข้อมูล**โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน**ได้อาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**
ระดับกลาง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับมาก**	**การแก้ไขหรือทำลายข้อมูล**โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรง**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน**ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรง**
ระดับสูง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับที่สุด**	**การแก้ไขหรือทำลายข้อมูล**โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน**ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**

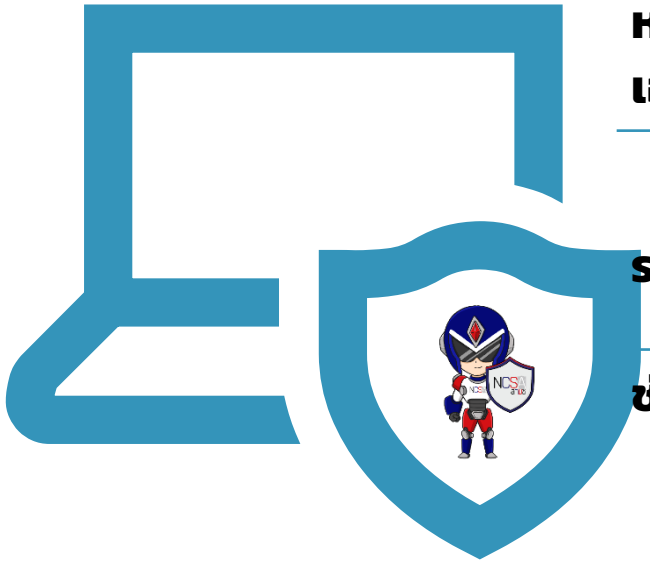
ผลกระทบระดับสูง **สูง**	ข้อกำหนดส่วนที่ ๑ - ทุกข้อ ข้อกำหนดส่วนที่ ๒ - ทุกข้อ	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓	ได้รับการรับรองโดยหน่วยงานให้บริการตรวจรับรอง (Certify Body) ตามวงรอบ ๓ ปี ประกอบด้วย การตรวจรับรองในปีที่ ๑ และการตรวจสำรวจในปีที่ ๒ และ ๓ และได้รับการรับรองตามมาตรฐาน ISO/IEC 27017 Certification หรือ CSA STAR Level 2/CCM และ ISO/IEC 27018 Certification และ ISO/IEC 27701 Certification เป็นอย่างน้อย

ตัวอย่างข้อมูลหรือระบบ “ระดับสูง” เช่น เอกสารลับที่สุด , ระบบทะเบียนราษฎร์, ข้อมูลส่วนบุคคลอ่อนไหว (ประวัติการรักษา, ข้อมูลชีวภาพ เป็นต้น)

Agenda

1. แนวทางการจัดการความปลอดภัยของระบบคลาวด์
2. NCSA Cloud Security Standard 2024
3. National Cloud Security Framework 2025

National Cloud Security Framework 2025 / กรอบมาตรฐานคลาวด์



คือแนวทางที่ สกมช. กำหนดขึ้นเพื่อรองรับการใช้งานคลาวด์ในหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและเอกชน

รองรับนโยบาย Cloud First Policy

ช่วยให้เกิดการเตรียมความพร้อมทั้งบุคลากร เทคโนโลยี และกระบวนการ

ครอบคลุมมาตรฐานความมั่นคงปลอดภัย เช่น ISO/IEC 27001, NIST 800-53c

ทำไมต้องทำกรอบมาตรฐานคลาวด์ฯ ขึ้นมา

- การใช้คลาวด์ในภาครัฐเพิ่มขึ้นอย่างรวดเร็ว
- ภัยคุกคามไซเบอร์มีความซับซ้อนมากขึ้น เช่น การโจมตีแบบ APT, ข้อมูลรั่วไหล
- สอดคล้องกับแนวทางการพัฒนาดิจิทัลของประเทศ
- ช่วยลดความเสี่ยงและเพิ่มความเชื่อมั่นในการใช้งานคลาวด์

ทำไมต้องทำกรอบมาตรฐานคลาวด์ฯ ขึ้นมา (ต่อ)

วัตถุประสงค์

- เพื่อผลักดันให้เกิดการดำเนินการ มาตรฐานคลาวด์ อย่างรวดเร็ว สะดวก และมีประสิทธิภาพ
- เพื่อยกระดับ Cloud Security ทั้งในส่วน Cloud Service Customer และ Cloud Service Provider
- เพื่อให้เกิดการบูรณาการระหว่าง สกมช. กับหน่วยงานที่เกี่ยวข้อง

ประโยชน์

- ลดความซ้ำซ้อน ความไม่สอดคล้องกัน และความไม่มีประสิทธิภาพในด้านต้นทุน
- สร้างความร่วมมือระหว่างภาครัฐ + เอกชน ด้าน Cloud Security
- ช่วยให้หน่วยงาน GOV. REG. และ CII นำระบบคลาวด์ มาใช้ โดยโปร่งใส บริหารความเสี่ยง Cloud Security

Reduce redundant efforts, inconsistencies, and cost inefficiencies

Strategy 1 : Public-Private Partnership

Strategy 2 : Promoting ecosystem

Strategy 3 : Capability building

Policy & responsible agencies

Stakeholders

Government agencies | Regulators | CIIs | Government cloud | Local cloud | Intl. cloud

Related frameworks

NIST CSF | ISO/IEC standards | CSA STAR | FedRAMP | Others (AUS, India)

แนวทางการทำงาน 5 ขั้นตอน

1. กำหนดความต้องการร่วม (Mutually requirements)
- 17 ความต้องการขั้นต้น

2. จัดลำดับความสำคัญ (Prioritize)
- สำรวจและแจ้งเวียนสรุปความต้องการขั้นต้น

3. จัดทำแผน (Plan)
- แผน 5 ปี เพื่อบูรณาการเพื่อขับเคลื่อน

4. ดำเนินการตามแผน (Execute)
- ตั้งทีมเฉพาะเพื่อประสานงาน

5. ประเมินผลอย่างต่อเนื่อง (Evaluate)

- ยุทธศาสตร์ที่ 1 รวมพลัง รัฐ + เอกชน
- ยุทธศาสตร์ที่ 2 สร้าง Eco System
- ยุทธศาสตร์ที่ 3 Capacity Building

ข้อเสนอแนะ, การดำเนินการสำคัญที่ผ่านมาของ สกมช.

	ดำเนินการแล้ว	กำลังจะดำเนินการ
ยุทธศาสตร์ที่ 1 รวมพลัง รัฐ + เอกชน	NoCSET	จัดทำแบบสอบถามเกี่ยวกับความพร้อมของหน่วยงาน
	INET Cloud Std. Mapping	AWS Cloud Std. Mapping
		Microsoft Cloud Std. Mapping
		BSA, SAP Cloud Standard Policy Roundtable Discussion 6 พ.ค. 2568
ยุทธศาสตร์ที่ 2 สร้าง Eco System	สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล (DTEC) และ วกรรมสถานแห่งประเทศไทย (วสท.)	พัฒนากลไกตรวจรับรอง และ เปิดบริการตรวจรับรอง
		ร่วมมือกับ CSA, ISO, NIST
ยุทธศาสตร์ที่ 3 Capacity Building	สกมช. จัดอบรม หลักสูตร Lead Auditor, Lead Implementer	Cloud Security Professional
	ช่องทางสอบถาม Q&A https://cloudsecurity.ncsa.or.th/	NCSA Cyber Clinic (SMART) 21 พ.ค. 68

Key Takeaways

ภาครัฐต้องศึกษาแนวทางการใช้ประโยชน์คลาวด์ทั้งในด้านการพัฒนา Cloud Native Application และมาตรฐาน Cloud Security Standard ของ สกมช.

เอกชน ต้องปรับตัวให้มีความพร้อมในการสนับสนุน Cloud First Policy และ Cloud Security Standard ของ สกมช.

ผู้ให้บริการ Cloud ในประเทศต้องเร่งยกระดับมาตราฐานในการบริการ

Q&A


TEAM
THAILAND
FOR CYBERTSECURITY

Contact us

National Cyber Security Agency - NCSA

NCSA Thailand

Line ID : NCSA Thailand

E-Mail:

saraban@ncsa.or.th

02-142-6885

shorturl.at/hkAC2

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

Security Categorization

ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567 | มีผลใช้บังคับ 18 มกราคม 2568 → มีผลบังคับใช้กับ GOV REG และ CII

เพื่อให้ GOV REG และ CII สามารถกำหนดความสำคัญของข้อมูล/ระบบสารสนเทศ นำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม ทำให้ประชาชนได้รับบริการที่มีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์อันจะส่งผลให้ธุรกิจหรือบริการภายในประเทศได้รับความน่าเชื่อมั่นมากยิ่งขึ้น อย่างคุ้มค่า

1 STEP กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

ให้แก่ข้อมูลหรือระบบสารสนเทศ **โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives)** ดังนี้

2 STEP ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น

โดยพิจารณาผลกระทบในแต่ละด้าน ดังนี้

3 STEP จัดระดับผลกระทบที่อาจเกิดขึ้นเป็น 3 ระดับ

ระดับต่ำ | ระดับกลาง | ระดับสูง

ระดับผลกระทบ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้องครบถ้วน (Integrity)	สภาพพร้อมใช้งาน (Availability)
ระดับต่ำ	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับ**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**
ระดับกลาง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับมาก**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรง**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรง**
ระดับสูง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับที่สุด**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**

หมายเหตุ

- **กรณีระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล** ให้กำหนดคุณลักษณะ โดย**ใช้ผลกระทบของข้อมูลที่มีระดับมากที่สุด**
- **หน่วยงานต้องพิจารณาทบทวนการกำหนดคุณลักษณะทุก 3 ปีเป็นอย่างน้อย** หรือทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานเปลี่ยนแปลงอย่างมีนัยสำคัญ

จัดทำโดย : สำนักกฎหมาย สกมช.

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7826
อีเมล : cii@ncsa.or.th

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

Security Baselines

ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567 | มีผลใช้บังคับ 18 มกราคม 2568 → มีผลบังคับใช้กับ GOV REG และ CII

เพื่อให้ GOV REG และ CII สามารถกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำได้อย่างเหมาะสมคุ่มค่า ลดมาตรการควบคุมและค่าใช้จ่ายที่เกินความจำเป็น ช่วยประหยัดงบประมาณแผ่นดินของประเทศ

ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ และได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว

ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

สำหรับข้อมูลหรือระบบสารสนเทศในแต่ละระดับ ดังนี้

- ผลกระทบระดับต่ำ = SET A
- ผลกระทบระดับกลาง = SET A + SET B
- ผลกระทบระดับสูง = SET A + SET B + SET C

	ประมวลแนวทางปฏิบัติ	กรอบมาตรฐานด้าน Cybersecurity
SET A	• **การประเมินความเสี่ยง** ด้าน Cybersecurity • **แผนการรับมือ** ภัยคุกคามทางไซเบอร์	• **การระบุความเสี่ยง** (Identify) – การจัดการทรัพย์สิน – การประเมินความเสี่ยงและกลยุทธ์ • **มาตรการตรวจสอบและเฝ้าระวัง** (Detect) – การตรวจสอบและเฝ้าระวัง • **มาตรการป้องกัน** (Protect) – การควบคุมการเข้าถึง – การทำให้ระบบมีความแข็งแกร่ง – การสร้างความตระหนักรู้ • **มาตรการเผชิญเหตุ** (Respond) – แผนการรับมือ – แผนการสื่อสารในภาวะวิกฤต – การฝึกซ้อม
SET B	• **แผนการตรวจสอบ** ด้าน Cybersecurity	• **มาตรการป้องกัน** (Protect) – การเชื่อมต่อระยะไกล – สื่อเก็บข้อมูลแบบถอดได้
SET C		• **การระบุความเสี่ยง** (Identify) – การประเมินช่องโหว่และการทดสอบเจาะระบบ – การจัดการผู้ให้บริการภายนอก • **มาตรการป้องกัน** (Protect) – การแบ่งปันข้อมูล • **มาตรการรักษาและฟื้นฟูความเสียหาย** (Recover) – การรักษาและฟื้นฟูความเสียหายที่เกิด

จัดทำโดย : สำนักกฎหมาย สกมช.

ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7826

อีเมล : cii@ncsa.or.th