ประชุมการรับฟังความคิดเห็น ร่างมาตรฐาน โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (Government Secure Infrastructure : GSI)

วันที่ ๒๗ สิงหาคม ๒๕๖๒

Agenda

๑. **มติการประชุม** คณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัล

๒. **ความก้าวหน้า** การดำเนินงานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

๓. **แนวทางและแผนการพัฒนา** โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย**ระยะ ๒ ปี** (**พ.ศ. ๒๕๖๒ – ๒๕๖๓**)

๔. **มาตรฐานและราคากลาง** ด้านโครงสร้างพื้นฐานดิจิทัลของหน่วยงานภาครัฐในปัจจุบัน

๕. **รูปแบบการกำกับดูแล** โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (Government Secure Intranet Governance Model)

๑. มติการประชุมคณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัล

เหตุผลความจำเป็น

ประชุมคณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัล **ครั้งที่ ๑/๒๕๖๑ เมื่อวันที่ ๙ มีนาคม ๒๕๖๑** โดยมี พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานในการประชุม

หน่วยงานภาครัฐ ขาดกระบวนการใน**การบริหารจัดการ**ด้าน IT Infrastructure **อย่างเป็นระบบ** ทำให้ไม่สามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ

บุคลากรภาครัฐ ที่มีทักษะและความเชี่ยวชาญ **มีไม่เพียงพอ** ที่จะรับมือภัยคุกคามและเทคโนโลยีใหม่ๆ

กระบวนจัดซื้อ และการจัดตั้งงบประมาณ มีข้อจำกัด ในด้านการจัดหาเทคโนโลยี บริการ อุปกรณ์ และวิธีการป้องกัน **ด้าน Cybersecurity ได้อย่างทันท่วงที** ยกตัวอย่างเช่น การตั้งงบประมาณล่วงหน้า

การลงทุนด้าน Cybersecurity มีค่าใช้จ่ายสูงโดยเฉพาะถ้าแต่ละหน่วยงานแยกบริหารจัดการเอง

Prominent Cybercriminal Business Models Over the Years

2018	Ransomware and DIGITAL EXTORTION will be the land of milk and honey for cybercriminals.
2017	Unprecedented ransomware outbreaks occur through WANNACRY and PETYA.
2016	New ransomware families spike by 752%, RANSOMWARE-AS-A-SERVICE (RaaS) emerges.
2015	Ransomware steadily grows, and continues to encrypt and demand payment.
2014	Ransomware BITCRYPT encrypts files and demands bitcoin payment.
2013	Ransomware CRYPTOLOCKER encrypts files, locks systems, and demands $300 payment.
2011	Trojan SPYEYE steals millions of dollars.
2010	First Android Trojan, DROIDSMS, emerges.
2009	Trojans spread via malicious links on Twitter.
2008	Worm KOOBFACE targets Facebook users. FAKEAV steals credit card information using fake antivirus scare messages.
2007	Infostealer ZEUS is discovered.
2004	Online banking malware that logs keystrokes or changes banking interfaces flourishes.

Prominent Cybercriminal Business Models Over The Years (ภาพจาก : Trend Micro)

แนวทางการขับเคลื่อน

มีมาตรการ แนวทาง ข้อปฏิบัติ ในการจัดการด้าน Cybersecurity ของภาครัฐ โดยต้องมีการบังคับใช้ และมีการตรวจสอบ เช่น การใช้งาน Internet, Intranet และอุปกรณ์ส่วนบุคคลที่นำมาใช้งานในองค์กร (Bring Your Own Device) เป็นต้น

เปลี่ยนแนวทางการจัดหาบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐ (Internet, Cloud เป็นต้น) ให้เป็นสาธารณูปโภค มอบภาระการดูแลด้าน Security ในส่วนเชื่อมต่อกับ Internet ให้เป็นหน้าที่ของผู้ให้บริการ GSI ที่ผ่านมาตรฐานการให้บริการที่กำหนด

สร้าง Government Secure Infrastructure (GSI) เพื่อเป็นโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัยในการเชื่อมโยงและเข้าถึงระบบสำคัญของภาครัฐ

มติการประชุมคณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัล ครั้งที่ ๑/๒๕๖๑

ที่ประชุม **มีมติเห็นชอบ** ในแนวทางการพัฒนารัฐบาลดิจิทัลดังกล่าว และให้รายงานคณะรัฐมนตรีทราบเพื่อให้เกิดการผลักดัน และดำเนินการต่อไป

โดยคณะรัฐมนตรีได้รับทราบมติดังกล่าวแล้ว ในการประชุมเมื่อ วันที่ ๑๙ มิถุนายน ๒๕๖๑

๒. ความก้าวหน้าการดำเนินงานโครงสร้างพื้นฐานดิจิทัลภาครัฐ ที่มีความมั่นคงปลอดภัย

แต่งตั้งคณะทำงานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

เพื่อให้การดำเนินการตามมติคณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัลดังกล่าว เป็นไปอย่างมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๒๙ และมาตรา ๓๐ แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. ๒๕๖๑ ผู้อำนวยการจึงเห็นสมควร**แต่งตั้งคณะทำงานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย** โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑.	นายรอม หิรัญพฤกษ์	ที่ปรึกษา
๒.	ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล	ประธานคณะทำงาน
๓.	ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	คณะทำงาน
๔.	ผู้แทนสำนักงบประมาณ	คณะทำงาน
๕.	ผู้แทนกรมบัญชีกลาง	คณะทำงาน
๖.	ผู้แทนสำนักงานคณะกรรมการพัฒนาระบบราชการ	คณะทำงาน
๗.	ผู้แทนสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	คณะทำงาน
๘.	ผู้แทนสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ	คณะทำงาน
๙.	นายกมล เอื้อชินกุล (หัวหน้างานรับรองคุณภาพบริภัณฑ์อิเล็กทรอนิกส์และคอมพิวเตอร์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)	คณะทำงาน
๑๐.	รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล	คณะทำงานและเลขานุการ
๑๑.	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ สำนักงานพัฒนารัฐบาลดิจิทัล	คณะทำงานและผู้ช่วยเลขานุการ

คำสั่งแต่งตั้งคณะทำงานฯ: หน้าที่และอำนาจ

๑.	จัดทำกรอบแนวทาง โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย
๒.	กำหนดเป้าหมาย และ หน่วยงานที่เกี่ยวข้อง ในการดำเนินการพัฒนาโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย รวมทั้งจัดลำดับความสำคัญของงานบริการเพื่อนำมาวางแผนการดำเนินงานในแต่ระยะ
๓.	จัดทำรายละเอียดคุณลักษณะเฉพาะ ของโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย ครอบคลุมการออกแบบสถาปัตยกรรมเทคโนโลยีสารสนเทศ (IT Architecture) ทั้งในด้านกระบวนการ ด้านระบบสารสนเทศ ด้านข้อมูล และด้านเทคโนโลยี และจัดทำเป็นข้อเสนอด้านเทคนิคต่อไป
๔.	จัดทำมาตรฐาน โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย เพื่อให้หน่วยงานของรัฐได้ใช้บริการกับผู้ให้บริการที่ผ่านมาตรฐานบริการดังกล่าว
๕.	จัดทำแนวทางการจัดหา โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย ให้เป็นแบบสาธารณูปโภค
๖.	พัฒนาต้นแบบ โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย
๗.	เชิญผู้แทน จากหน่วยงานของรัฐหรือบุคคลที่เกี่ยวข้อง เพื่อให้ข้อมูลหรือข้อเสนอแนะตามความเหมาะสม
๘.	ดำเนินการอื่นใดที่เกี่ยวข้อง ตามความจำเป็นและเหมาะสม

ผลการประชุมคณะทำงานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

ครั้งที่ ๑/๒๕๖๒

เมื่อวันที่ ๙ มกราคม ๒๕๖๒

- รับทราบ ความก้าวหน้าในการหารือหน่วยงานที่เกี่ยวข้องด้านมาตรฐาน โดย สพร. ดำเนินการในส่วนของมาตรฐานด้านเครือข่าย ส่วนมาตรฐานระบบคลาวด์และมาตรฐานศูนย์ข้อมูลให้ประยุกต์มาตรฐานที่ “คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)” เป็นผู้จัดทำ
- เห็นชอบแผนการพัฒนาโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (GSI Roadmap) และให้นำข้อเสนอแนะไปพิจารณาประกอบการดำเนินงาน
- เห็นชอบ (ร่าง) มาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (GSI Common Standard)
- เห็นชอบ (ร่าง) มาตรฐานบริการเครือข่ายภาครัฐที่มีความมั่นคงปลอดภัย (GSI Network Standard)

ครั้งที่ ๒/๒๕๖๒

เมื่อวันที่ ๑๔ กุมภาพันธ์ ๒๕๖๒

- เห็นชอบร่าง มาตรฐานเครือข่ายที่มีความมั่นคงปลอดภัย (GSI Network Standard) และแนวทางการทำประชาพิจารณ์
- รับทราบ แนวทางการดำเนินการด้านมาตรฐานของคณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อเป็นประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)
- รับทราบ แนวทางการใช้งาน IPv6 ในโครงสร้างพื้นฐานดิจิทัลภาครัฐ ที่มีความมั่นคงปลอดภัย

ผลการประชุมคณะทำงานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (ต่อ)

ครั้งที่ ๓/๒๕๖๒

เมื่อวันที่ ๒๗ มิถุนายน ๒๕๖๒

- รับทราบ การเปลี่ยนแปลงเลขานุการในส่วนของตำแหน่งเลขานุการ และผู้ช่วยเลขานุการ
- พิจารณา (ร่าง) มาตรฐานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย
- ขอความเห็นเพิ่มเติมเพื่อปรับปรุง (ร่าง) มาตรฐานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย และไม่มีความเห็นเพิ่มเติมจากคณะทำงานจึงนำมาสู่การประชุมประชาพิจารณ์
- เริ่มดำเนินการกับหน่วยงานนำร่อง จำนวน 10 หน่วยงานตามแผนการดำเนินการ โดยมีหน่วยงานเข้าร่วมเป็นหน่วยงานนำร่องดังต่อไปนี้

<u>หน่วยงานนำร่อง</u>

1. กรมเจ้าท่า
2. สำนักงานตำรวจแห่งชาติ
3. กรมพัฒนาธุรกิจการค้า
4. กองทัพบก (กอ.รมน. ภาค 4)
5. ศูนย์บริการโลหิตแห่งชาติ
6. สำนักงานหลักประกันสุขภาพแห่งชาติ
7. สำนักงานอัยการสูงสุด
8. กองทัพอากาศ
9. กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
10. กรมธนานุเคราะห์

๓. แนวทางและแผนการพัฒนาโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย ระยะ ๒ ปี (พ.ศ. ๒๕๖๒ – ๒๕๖๓)

วัตถุประสงค์

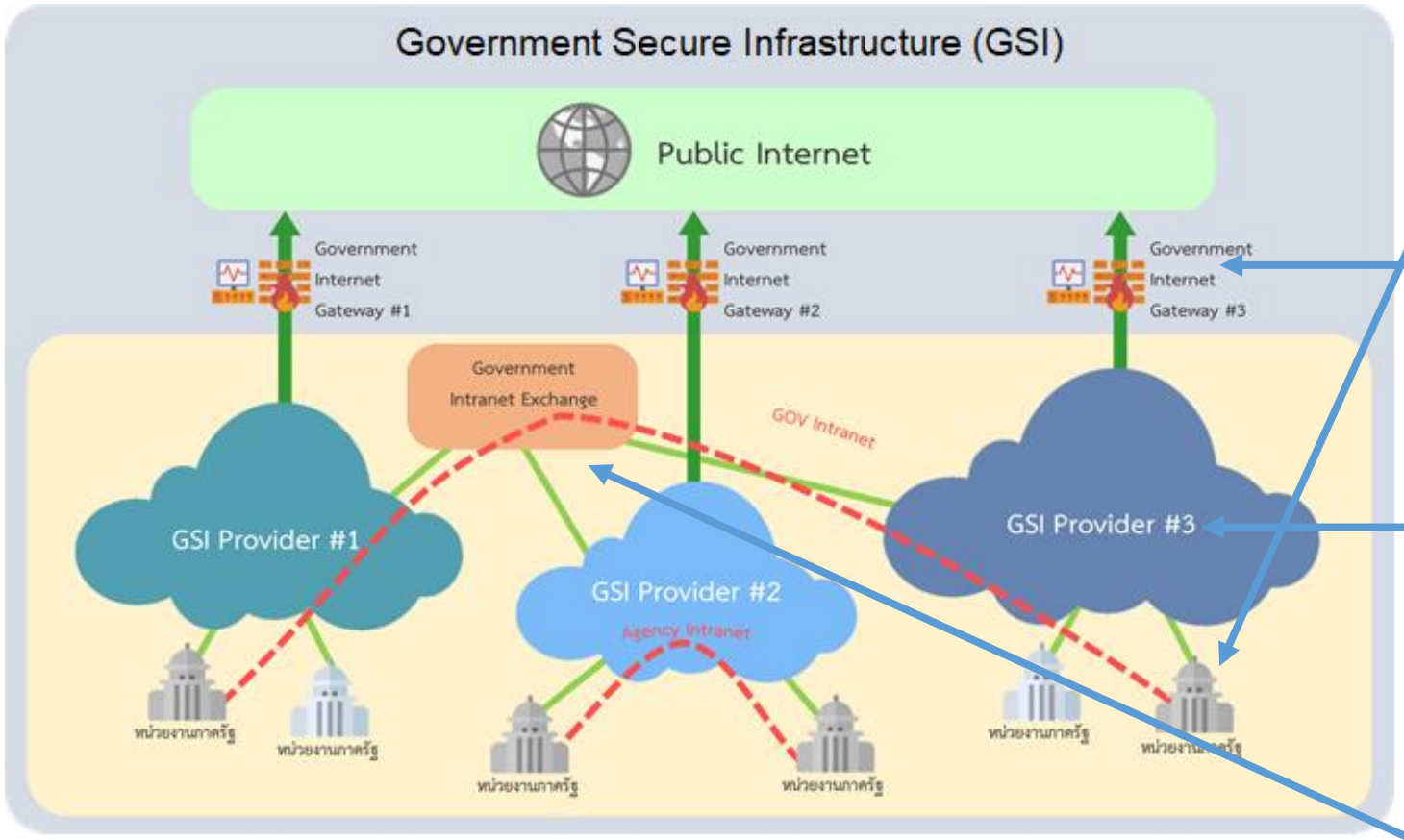
เพิ่มศักยภาพ	ด้านดิจิทัลของประเทศ
ยกระดับบริการ	ด้านดิจิทัลของหน่วยงานภาครัฐ
ให้บริการที่เป็นมาตรฐาน	มีความมั่นคงปลอดภัย ให้บริการได้อย่างต่อเนื่อง
ใช้งบประมาณอย่างคุ้มค่า	เพิ่มประสิทธิภาพการใช้งบประมาณ
เกิดการสร้างโอกาส	การมีส่วนร่วม การรับบริการที่มีคุณภาพจากผู้ให้บริการ

สะดวก พร้อมใช้ ปลอดภัย น่าเชื่อถือ

กรอบแนวทางการพัฒนา

๑.	สถาปัตยกรรม	โครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย ผู้รับผิดชอบ คณะทำงานโครงสร้างฯ
๒.	กำหนดมาตรฐาน	ที่เกี่ยวข้องกับโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย ผู้รับผิดชอบ คณะทำงาน/หน่วยงานภาครัฐ
๓.	กำหนดราคากลาง	ของบริการที่เกี่ยวข้องกับโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย ผู้รับผิดชอบ คณะกรรมการกำหนดราคากลาง (เช่น สพร., กรมบัญชีกลาง, สำนักงบประมาณ, ผู้ให้บริการ)
๔.	คัดเลือกผู้ให้บริการ	ที่ผ่านมาตรฐานการให้บริการโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย ผู้รับผิดชอบ คณะกรรมการคัดเลือกผู้ให้บริการ (เช่น สพร., กรมบัญชีกลาง)
๕.	ปรับเปลี่ยนแนวทาง	การจัดหาบริการโครงสร้างพื้นฐานดิจิทัลภาครัฐ ให้เป็นแบบสาธารณูปโภค ผู้รับผิดชอบ สพร., กรมบัญชีกลาง
๖.	มีหน่วยงานนำร่อง	ตามแนวทางการพัฒนาความมั่นคงปลอดภัยโครงสร้างพื้นฐานดิจิทัล ผู้รับผิดชอบ สพร., หน่วยงานภาครัฐ
๗.	ขยายผลหน่วยงานภาครัฐ	ตามแนวทางการพัฒนาความมั่นคงปลอดภัยโครงสร้างพื้นฐานดิจิทัล ผู้รับผิดชอบ สพร., หน่วยงานภาครัฐ

แนวคิดการออกแบบ GSI - Network



หน่วยงานภาครัฐ สามารถ**ใช้บริการ**กับผู้ให้บริการ**ที่ผ่านมาตรฐานที่กำหนด** (GSI Provider)

Government Internet Gateway

อยู่ที่ผู้ให้บริการ และ**ผู้ให้บริการ** เป็นผู้**ดูแลด้าน Cybersecurity**

ผู้ให้บริการ (GSI Provider) ต้อง**ตั้งค่า**บริการ**ให้**สามารถ**เชื่อมโยง**ระหว่าง

- **ภายใน**หน่วยงานเดียวกัน (Agency Intranet)
- **ข้าม**หน่วยงาน (Government Intranet)

Government Intranet eXchange

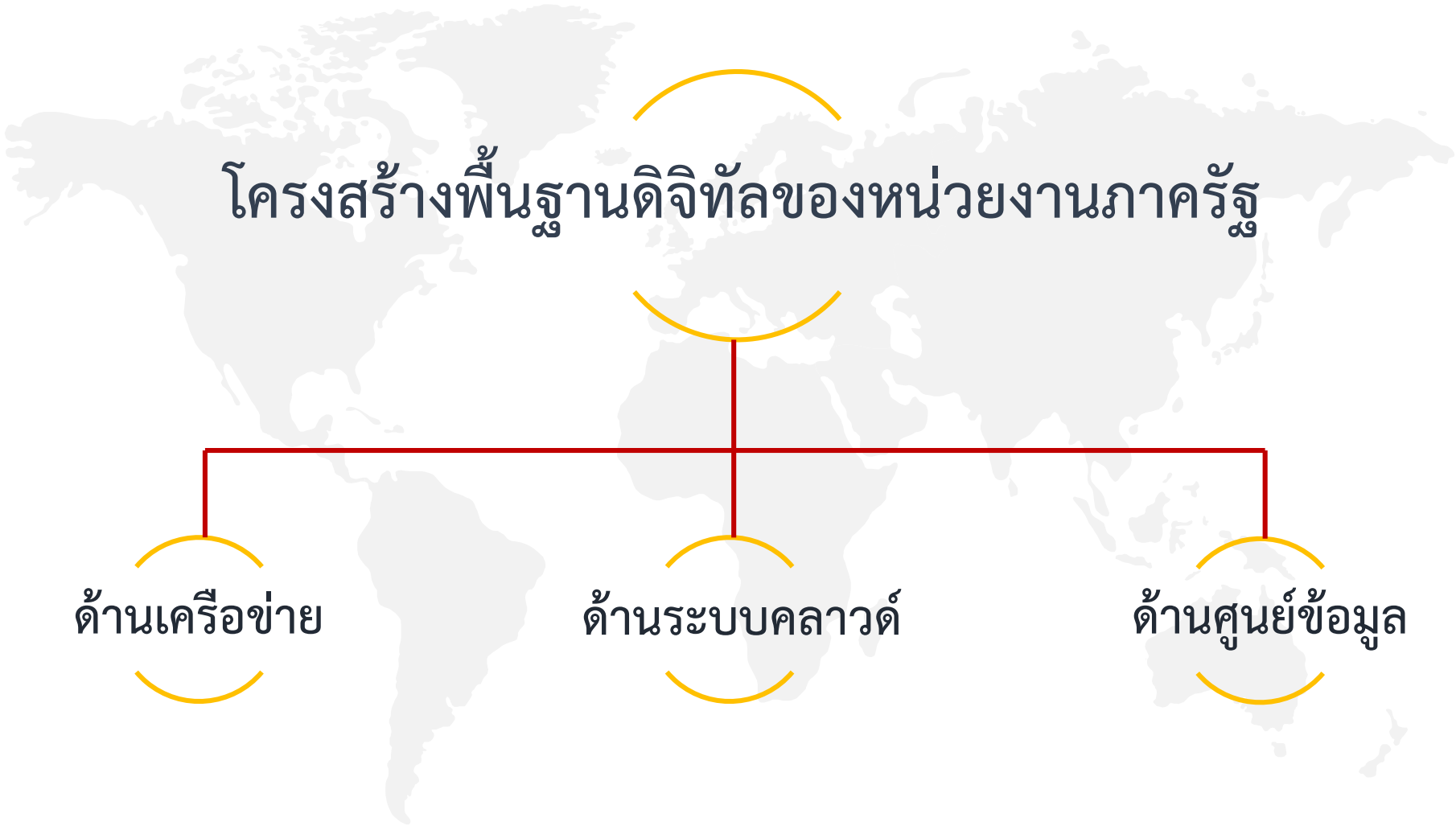
จะเป็นจุด**เชื่อมโยง** ของ **ทุก** GSI Provider

แผนการนำร่องและขยายผลการดำเนินการ

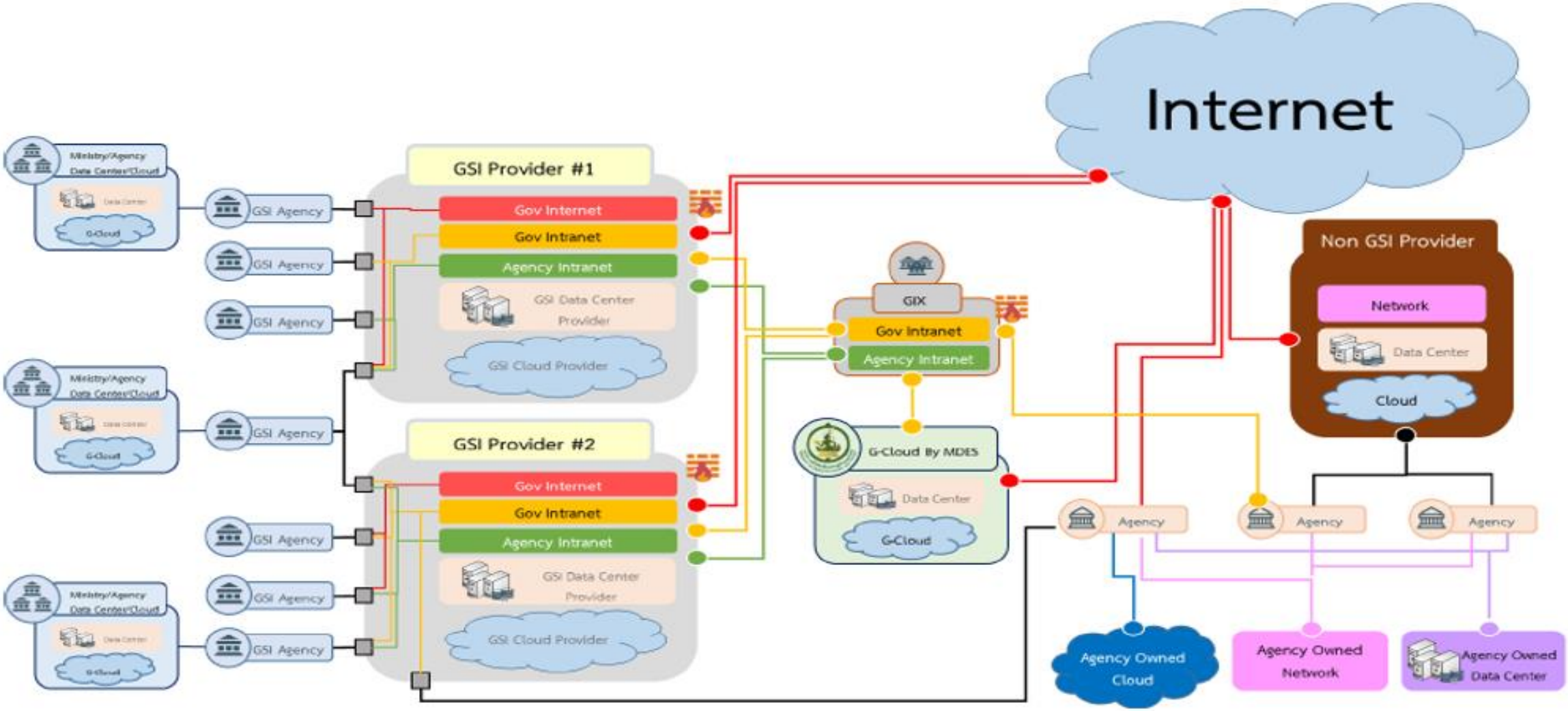
แผนการดำเนินงาน	ม.ค. – มี.ค. ๒๕๖๒	เม.ย. – มิ.ย. ๒๕๖๒	ก.ค. – ก.ย. ๒๕๖๒	ต.ค. – ธ.ค. ๒๕๖๒	ม.ค. – มี.ค. ๒๕๖๓
นำร่อง	• คัดเลือกผู้ให้บริการ • คัดเลือกผู้ใช้บริการ ๑๐ หน่วยงาน • คัดเลือกผู้ตรวจสอบ	นำร่องโครงการ GSI		• ตรวจประเมินผู้ให้บริการตามมาตรฐาน ช่วงนำร่อง • สรุปผลจากหน่วยงานนำร่อง	
ขยายผลการดำเนินการ	(ร่าง) มาตรฐาน (ร่าง) แนวทางการจัดหาบริการ (ราคากลาง, การจัดซื้อจัดจ้าง, การตรวจรับ)	ติดตามมาตรฐานที่เกี่ยวข้องเพื่อนำมาใช้ในโครงการ กำหนดแนวทางการจัดหาบริการ	ประชาพิจารณ์ (ร่าง) มาตรฐานเครือข่าย ประกาศใช้มาตรฐาน กำหนดราคากลาง จัดทำ TOR Template	ประชาสัมพันธ์เพื่อสร้างความรู้และความเข้าใจ คัดเลือกผู้ตรวจประเมิน และจัดทำรายชื่อผู้ตรวจประเมิน คัดเลือกผู้ให้บริการ และจัดทำรายชื่อผู้ให้บริการ GSI จัดทำตัวอย่างคำของบประมาณสำหรับปีงบประมาณ 2564	ปรับปรุงรายละเอียดต่างๆ ที่เกี่ยวข้องจากผลที่ได้จากการนำร่องโครงการ ขยายผลโครงการ GSI

๔. สถาปัตยกรรม มาตรฐาน และราคากลาง ด้านโครงสร้างพื้นฐานดิจิทัลของหน่วยงานภาครัฐ

โครงสร้างพื้นฐานดิจิทัลของหน่วยงานภาครัฐ



สถาปัตยกรรมโครงสร้างพื้นฐานดิจิทัลของหน่วยงานภาครัฐ



มาตรฐานด้านโครงสร้างพื้นฐานดิจิทัลที่มีในปัจจุบัน

บริการ	มาตรฐาน	หน่วยงาน
ด้านเครือข่าย (Network)	ยังไม่มีหน่วยงานจัดทำ	
ด้านระบบคลาวด์ (Cloud)	มาตรฐานและแนวทางปฏิบัติการออกแบบโครงสร้างพื้นฐานทางด้านสารสนเทศเพื่อการประมวลผลข้อมูลภาครัฐ	คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)
	หลักเกณฑ์การให้บริการ Cloud Computing	สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
	มาตรฐานปฏิบัติการบริการแบบคลาวด์ Cloud Services Standard of Practice ฉบับเทคนิคพิจารณ์	วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
	นโยบายโครงสร้างพื้นฐานบนอินเทอร์เน็ตแบบใช้ทรัพยากรร่วมกัน (Cloud Policy) ในการให้บริการภาครัฐ ภาคเอกชน	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
	มาตรฐานความมั่นคงปลอดภัยการให้บริการเทคโนโลยีสารสนเทศระบบคลาวด์ภาครัฐ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ด้านศูนย์ข้อมูล (Data Center)	มาตรฐานดาตาเซนเตอร์สำหรับประเทศไทย	วิศวกรรมสถานแห่งประเทศไทย ในพระบรมราชูปถัมภ์ (วสท.)
	(ร่าง) มาตรฐานและแนวทางปฏิบัติการออกแบบโครงสร้างพื้นฐานด้านสารสนเทศเพื่อการประมวลผลข้อมูลภาครัฐ	คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing)
	(ร่าง) มาตรฐานบริการศูนย์ข้อมูลภาครัฐ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

เกณฑ์ราคากลาง ณ ปัจจุบัน

บริการ	เกณฑ์ราคากลาง	ผู้กำหนดราคากลาง
ด้านเครือข่าย (Network)	ยังไม่มีหน่วยงานจัดทำ	
ด้านระบบคลาวด์ (Cloud)	เกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ ประจำปี พ.ศ. 2562 67. ค่าเช่าระบบ Cloud Server แบบที่ 1 ราคา 6,500 บาทต่อเดือน (ราคาค่าเช่านี้ไม่รวมราคาการให้บริการรับส่งข้อมูล (Data Transfer) เข้าสู่ระบบ) 68. ค่าเช่าระบบ Cloud Server แบบที่ 2 ราคา 18,000 บาทต่อเดือน (ราคาค่าเช่านี้ไม่รวมราคาการให้บริการรับส่งข้อมูล (Data Transfer) เข้าสู่ระบบ)	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ด้านศูนย์ข้อมูล (Data Center)	เกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ ประจำปี พ.ศ. 2562 66. ค่าเช่าพื้นที่ตู้ Rack สำหรับวางระบบคอมพิวเตอร์ (Rack Data Center Co-location) ขนาดไม่น้อยกว่า 42U ราคา 40,000 บาทต่อเดือน	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

แนวทางการจัดทำมาตรฐานและเกณฑ์ราคากลางด้านโครงสร้างพื้นฐานดิจิทัลของหน่วยงานภาครัฐ

มาตรฐานและเกณฑ์ราคากลาง

ด้านเครือข่าย

(ภายใต้ คณะกรรมการรัฐบาลดิจิทัล)

มาตรฐานบริการเครือข่าย
ที่มีความมั่นคงปลอดภัย

ด้านระบบคลาวด์

ด้านศูนย์ข้อมูล

(ภายใต้ คณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing))

มาตรฐานและแนวทางปฏิบัติการออกแบบโครงสร้างพื้นฐาน
ด้านสารสนเทศเพื่อการประมวลผลข้อมูลภาครัฐ

หลักการ การเชื่อมโยงเครือข่ายดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (GSI - Network)

เครือข่าย GSI เป็นเครือข่ายอินทราเน็ตภาครัฐที่เชื่อมต่อกับทุกหน่วยงานด้วยมาตรฐานความมั่นคงปลอดภัยสูง ที่ให้บริการโดยเอกชน หรือรัฐวิสาหกิจ (เรียกว่า “GSI Provider”) โดยมีการกำหนดนโยบาย และมาตรฐานการให้บริการ โดยเป็นเครือข่ายที่มีการจัดการอย่างเป็นระบบและสามารถรองรับการใช้งานได้อย่างเพียงพอ

๑. **มีการกำหนดมาตรฐาน** ความมั่นคงปลอดภัยทั้งในส่วนการบริหารจัดการเครือข่าย การควบคุมการเชื่อมต่อกับอุปกรณ์ปลายทาง (End to End security) รวมถึงอุปกรณ์ส่วนบุคคลที่นำมาใช้งานในองค์กร (Bring your own device)

๒. **ให้บริการอย่างเพียงพอเช่นเดียวกับการบริการด้านสาธารณูปโภค** สามารถปรับเพิ่มลดความเร็ววงจรตามความต้องการใช้งานในแต่ละช่วงเวลาได้

๓. **มี Government Intranet eXchange (GIX)** เพื่อรองรับการแลกเปลี่ยนข้อมูลผ่านเครือข่ายของผู้ให้บริการ

๔. **มีการกำหนดมาตรฐานการให้บริการเครือข่าย แคตตาล็อคบริการ** (Specification, SLA, Standard Price) และ**เกณฑ์การคัดเลือกผู้ให้บริการ** (GSI Provider List) เพื่อเปิดโอกาสให้เอกชน หรือรัฐวิสาหกิจเป็นผู้ให้บริการตามมาตรฐานและกติกาที่ภาครัฐกำหนด

๕. **มีระบบกลางสำหรับหน่วยงานในการตรวจสอบ** วิเคราะห์ ปริมาณการใช้งาน รวมถึง แจ้งปัญหาการใช้บริการเครือข่าย และภัยคุกคาม โดยที่ผู้ใช้งานสามารถเข้าดูได้เอง

๖. **มีการวิเคราะห์ปริมาณการใช้งานสูงสุดของแต่ละหน่วยงานเป็นรายปี** เพื่อเป็นข้อมูลประมาณการงบประมาณที่ต้องเตรียมไว้สำหรับแต่ละหน่วยงาน โดยใช้วิธีการตั้งงบประมาณแบบรวมศูนย์ และชำระค่าใช้บริการตามปริมาณการใช้งานจริงของแต่ละหน่วยงาน

๗. **มีหน่วยงานทำหน้าที่ติดตามและกำกับของแนวทางการให้บริการ** Government Secure Intranet (GSI)

สถาปัตยกรรมการเชื่อมโยงเครือข่ายดิจิทัลภาครัฐ

รูปแบบและกรอบการดำเนินงานสำหรับการบริหารจัดการเครือข่ายด้วย FCAPS

Fault Management

- การตรวจสอบสถานะของระบบคอมพิวเตอร์ และเครือข่าย
- การตรวจสอบปัญหาและการแจ้งปัญหา
- การวิเคราะห์ถึงเหตุของปัญหา
- การแก้ไขปัญหา
- การบันทึกปัญหา และวิธีการแก้ไข

Security Management

- การควบคุมการเข้าถึงทรัพยากรต่างๆ ของระบบเครือข่าย (ACL)
- การจัดตั้งนโยบายรักษาความปลอดภัยการใช้งานเครือข่ายคอมพิวเตอร์
- มีการนำระบบ AAA (Authentication, Authorization, Accounting) เข้ามาใช้งาน
- มีการตรวจสอบบันทึกการเข้าถึง (Logging) อย่างสม่ำเสมอ
- การทำ Data Encryption

Configuration Management

- ลักษณะการเชื่อมต่อ และความสัมพันธ์ต่างๆ ของระบบ
- ข้อมูลต่างๆ ของอุปกรณ์ เช่น รุ่น ยี่ห้อ คุณลักษณะ ซอฟต์แว
- ข้อมูล Configuration ต่างๆ ที่ทันสมัยอยู่ตลอดเวลา
- การทำ Change Management
- การเข้าถึงข้อมูลที่สำรองไว้อย่างรวดเร็ว

Performance Management

- การดำเนินการเพื่อให้ระบบเครือข่ายสามารถใช้ได้อย่างเต็มประสิทธิภาพ
- สิ่งที่จำเป็นจะต้องคำนึงถึง: Throughput, Utilization, Error, Response Time
- มีการกำหนดค่ามาตรฐานในการใช้งานเครือข่าย
- มีระบบเตือนผู้ดูแลหากมีการใช้งานเกินค่ามาตรฐานดังกล่าว เพื่อให้มีการดำเนินการอื่นๆ ต่อไป

Accounting Management

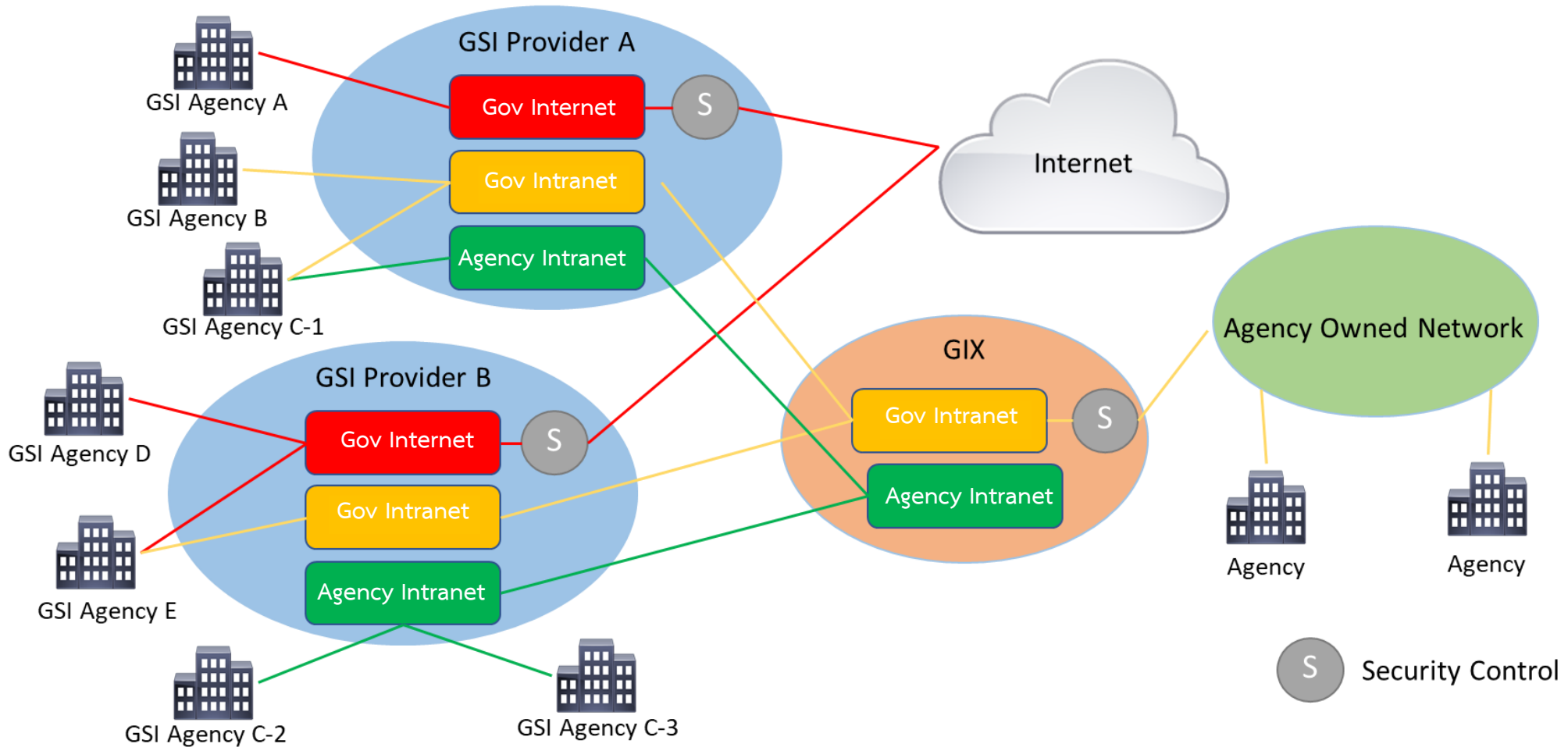
- การบันทึกกิจกรรมต่างๆ ในระบบเครือข่าย
- การคำนวณต้นทุนในการใช้งานระบบเครือข่าย
- การดำเนินการเพื่อลดต้นทุน การกำหนดนโยบาย หรือ Quota ในการใช้งาน

รูปแบบการเชื่อมโยงเครือข่าย

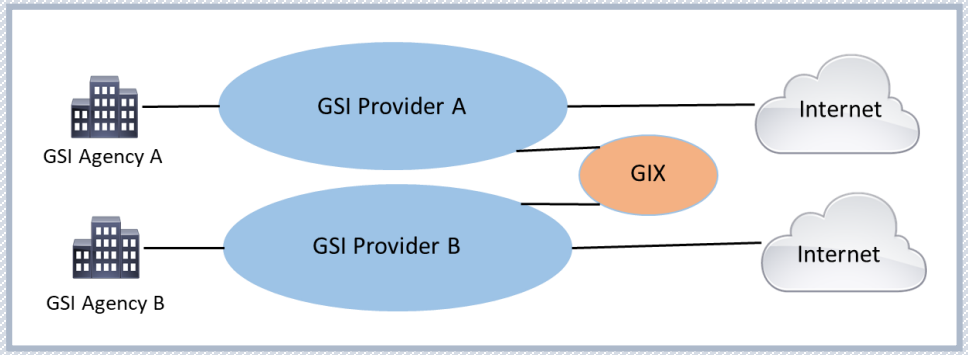
- **GSI Agency** เชื่อมต่อหน่วยงานและสาขาต่างๆ ภายในกรมเดียวกัน ผ่านการให้บริการของ GSI Provider **ในลักษณะ Agency Intranet**
- **GSI Agency** เชื่อมต่อหน่วยงานระหว่างหน่วยงานระดับกรม/กระทรวง ผ่านการให้บริการของ GSI Provider **ในลักษณะ Government Intranet** ตามวัตถุประสงค์ของงานนั้นๆ เช่น NSW, GFMIS และ DOPA เป็นต้น
  - ผ่านทางส่วนงานกลาง (HQ)
- **GSI Agency** ใช้บริการ Internet (Domestic/International) ผ่านการให้บริการ GSI Provider ได้ ๒ ลักษณะ คือ
  - ผ่านทางส่วนงานกลาง (HQ)
  - หน่วยงานสาขาสามารถใช้งาน Internet ผ่านทาง GSI Provider ได้โดยตรง

- **GSI Provider** จะต้องรองรับการให้บริการที่มีความปลอดภัยในการให้บริการตามมาตรฐานที่กำหนด
- **Government Intranet eXchange (GIX)** เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลของ GSI Agency ระหว่าง GSI Provider ที่ต่างกัน

รูปแบบการเชื่อมโยงเครือข่าย



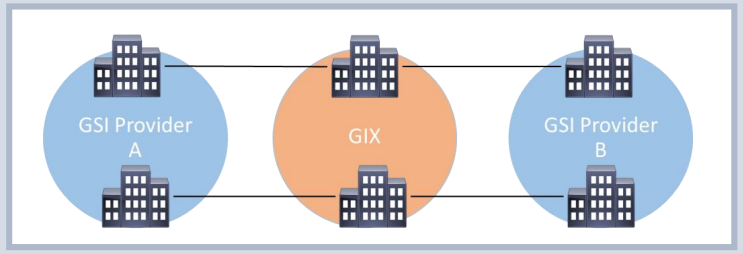
รูปแบบการเชื่อมโยงเครือข่าย



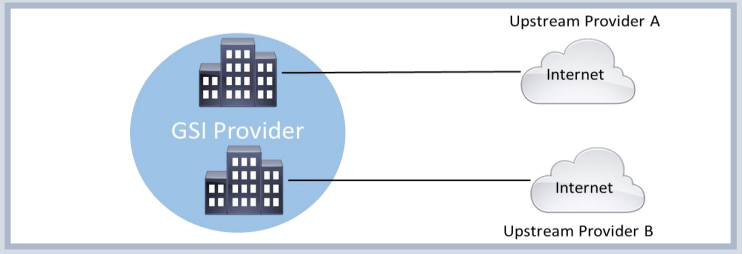
การเชื่อมต่อ ในภาพรวมของเครือข่าย GSI

การเชื่อมต่อ GSI Agency และ GSI Provider

การเชื่อมต่อ ระหว่าง GSI Provider



การเชื่อมต่อ GSI Provider และ Internet



(ร่าง) มาตรฐานบริการเครือข่ายที่มีความมั่นคงปลอดภัย (GSI Network Standard)

- ความต้องการทั่วไป
- ความต้องการทางเทคนิค
- ข้อกำหนดระดับการให้บริการ

รูปแบบและแนวทางการเชื่อมโยงเครือข่าย	• การเชื่อมต่อระหว่าง GSI Agency และ GSI Provider รูปแบบต่างๆ • การปฏิบัติตามข้อกำหนดของคุณลักษณะ GSI Provider • การเชื่อมต่อระหว่าง GSI Provider และ GSI Intranet eXchange (GIX)
การปฏิบัติตามกฎหมายและมาตรฐาน	• กฎหมายด้านเทคโนโลยีสารสนเทศ และด้านโทรคมนาคม • มาตรฐานสากล เช่น ISO20000, ISO22301 และ ISO27001
ประสิทธิภาพของบุคลากร	• ทักษะและความสามารถของบุคลากร • ต้องได้รับการตรวจสอบประวัติอาชญากรรม • มีขั้นตอนการปฏิบัติงานเกี่ยวกับการรักษาความลับและเปิดเผยข้อมูล
ประสิทธิภาพสำหรับให้บริการ	• ความสามารถในการให้บริการ (Capacity) • การเชื่อมโยงเครือข่ายการใช้หมายเลข IPv4 และ IPv6 • ระบบสำรองฉุกเฉิน
การให้บริการ	• การเชื่อมโยงเครือข่ายระหว่าง GSI Provider ไปยัง GSI Agency และ GIX • รูปแบบการให้บริการ, SLA, การบริการพื้นฐานด้านเครือข่าย เช่น DNSSEC, NTP, Security • ระบบบริการตนเองสำหรับ GSI Agency
ระดับการให้บริการ การปฏิบัติการและการบริหารจัดการ	• มีระบบเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศและการเชื่อมโยงเครือข่าย • การรับแจ้งปัญหา • การจัดทำรายงาน

(ร่าง) มาตรฐานรัฐบาลดิจิทัล เครือข่ายคอมพิวเตอร์ภายในภาครัฐที่มีความมั่นคงปลอดภัย - ข้อกำหนดด้านเครือข่าย

เนื้อหาโดยสังเขป

- ขอบข่าย, บทนิยาม และเอกสารอ้างอิง
- ข้อกำหนดที่ต้องการทั่วไป
  - ✓ ข้อกำหนดทั่วไปของผู้ให้บริการ
  - ✓ ข้อกำหนดด้านการบริหารองค์กร
  - ✓ ทรัพยากร
  - ✓ บันทึก ข้อมูลและรายงาน
- ข้อกำหนดด้านเครือข่าย
- การประเมินระดับการให้บริการ
- ภาคผนวก ก ข้อยกเว้น ต่อระดับการให้บริการ
- ภาคผนวก ข การทดสอบ การประเมินผล และเกณฑ์ระดับการให้บริการของผู้ให้บริการเครือข่าย

GSI Provider ต้องดำเนินการตามมาตรฐานที่กำหนด

ระบุใน ข้อ 4. ข้อกำหนดที่ต้องการทั่วไป

ข้อกำหนดทั่วไป ต้องปฏิบัติตามกฎหมายต่าง ๆ ที่เกี่ยวข้อง โดยเฉพาะ กฎหมายด้านเทคโนโลยีสารสนเทศ และ กฎหมายด้านโทรคมนาคม

ข้อกำหนดด้านการบริหารองค์กร

- ระบบจัดการงานบริการด้านเทคโนโลยีสารสนเทศต้องสอดคล้องกับมาตรฐาน ISO/IEC 20000-1
- ระบบบริหารความต่อเนื่องทางธุรกิจต้องสอดคล้องกับมาตรฐาน มอก. 22301 หรือ ISO 22301
- ระบบบริหารความมั่งคงปลอดภัยสารสนเทศต้องสอดคล้องกับมาตรฐาน มอก. 27001 หรือ ISO/IEC 27001

ทรัพยากร คุณสมบัติของบุคลากรของผู้ให้บริการ และ ผู้รับเหมา

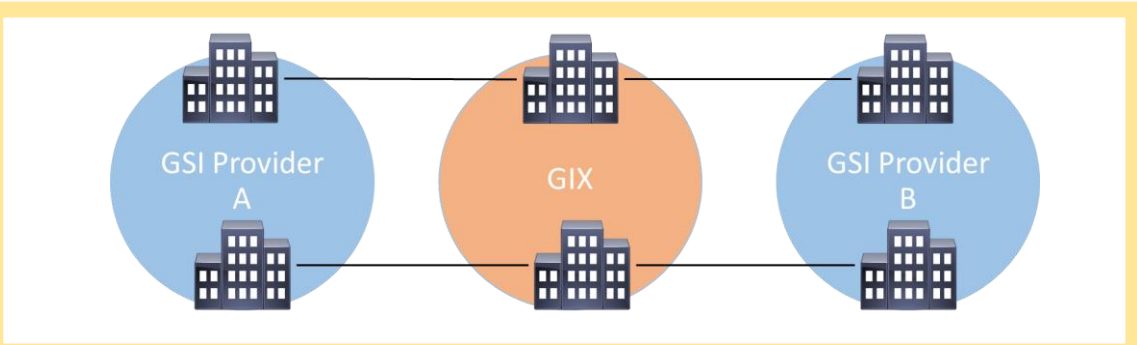
บันทึก ข้อมูลและรายงาน

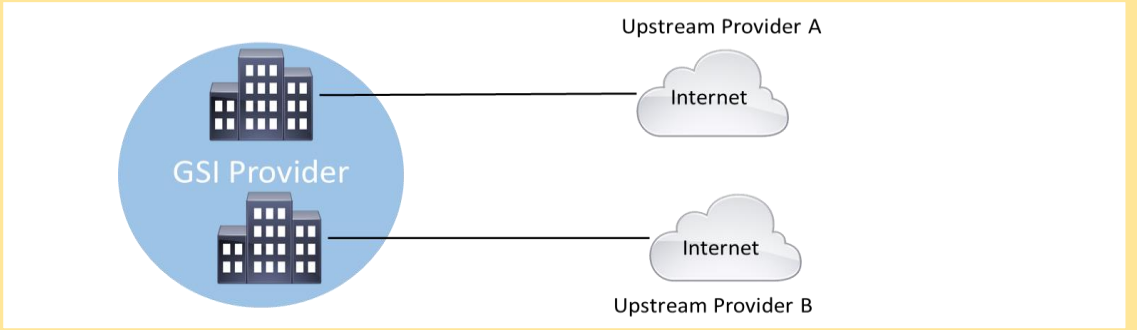
- ต้องกำหนดนโยบายและขั้นตอนการปฏิบัติงานเป็นลายลักษณ์อักษรเกี่ยวกับการรักษาความลับและการเปิดเผยข้อมูล
- ต้องมีระบบจัดเก็บบันทึกข้อมูลในรูปแบบดิจิทัล
- ต้องมีระบบเฝ้าระวัง วิเคราะห์และชี้บ่งเหตุ ได้ทั้งในลักษณะทันทีหลังเกิดเหตุ และต้องสามารถจัดทำรายงานได้
- ต้องสามารถจัดทำรายงานค่าใช้บริการพร้อมรายละเอียดการใช้บริการเพิ่มเติมได้

GSI Provider ต้องดำเนินการตามมาตรฐานที่กำหนด - ข้อกำหนดด้านเครือข่าย

Routing

- GSI Provider ต้องมีเครือข่ายเชื่อมต่อมา GIX เพื่อแลกเปลี่ยนข้อมูลไปยังผู้ให้บริการรายอื่น >= 2 เส้นทาง และแต่ละเส้นทางต้องมีปริมาณการใช้งานเฉลี่ย ในรอบเดือน < 75% ของแบนด์วิดท์สูงสุดในแต่ละวงจร
- GSI Intranet eXchange (GIX) เป็นผู้กำหนด IP Address ให้ GSI Provider
- GSI Provider ต้องมีระบบสำรองในกรณีฉุกเฉินหรือเกิดเหตุภัยพิบัติต่าง ๆ เพื่อให้ระบบสามารถบริการได้อย่างต่อเนื่อง
- GSI Provider ต้องมีการเชื่อมต่อไปยัง NIX >= 2 ช่องทาง
- GSI Provider ต้องมีการเชื่อมต่อไปยัง Upstream Provider >= 2 ราย สำหรับบริการ Int'l Internet และต้องมีอัตราการใช้งานเฉลี่ย ในรอบเดือน < 85% ของขนาดแบนด์วิดท์รวมทั้งหมดของผู้ให้บริการ





Security and Availability

- GSI Provider ต้องมีบริการเครือข่ายพื้นฐาน ได้แก่ DNSSEC, NTP เป็นต้น
- GSI Provider ต้องมีการให้บริการด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ไฟร์วอลล์ (Firewall), IDS/IPS, WAF และ DOS/DDOS Protection
- GSI Provider ต้องประกาศแจ้ง ระดับการให้บริการ (Service Availability) ที่มีให้แก่ผู้ใช้บริการทราบ

เกณฑ์ระดับการให้บริการของ GSI Provider

ระดับการให้บริการของวงจรสื่อสาร Last mile-แบ่งตามประเภทของพื้นที่ในการให้บริการ

ระดับคุณภาพและประสิทธิภาพของวงจรสื่อสาร Last mile

- Latency เฉลี่ย < 25ms
- Packet loss < 2%

ระดับการให้บริการของวงจรสื่อสารมายัง GIX-ไม่น้อยกว่า 99.95%

ระดับการให้บริการของวงจรสื่อสารมายัง Domestic Internet-ไม่น้อยกว่า 99.95%

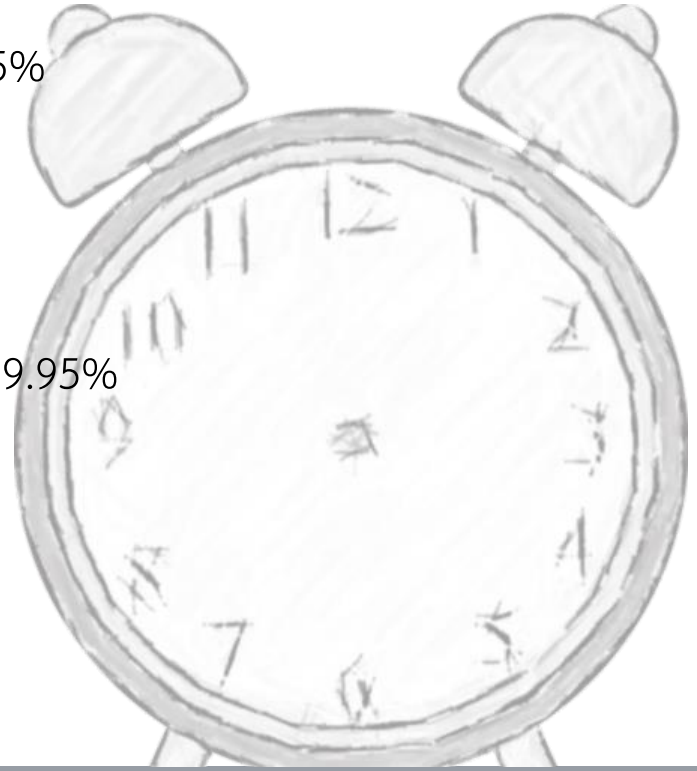
ระดับคุณภาพและประสิทธิภาพของวงจรสื่อสาร Domestic Internet

- Latency เฉลี่ย < 20ms
- Packet loss < 2%

ระดับการให้บริการของวงจรสื่อสารมายัง International Internet-ไม่น้อยกว่า 99.95%

ระดับคุณภาพและประสิทธิภาพของวงจรสื่อสาร Domestic Internet

- Latency เฉลี่ย ไปยังประเทศสิงคโปร์ < 100ms
- Latency เฉลี่ย ไปยังประเทศสหรัฐอเมริกาฝั่งตะวันตก < 300ms
- Packet loss < 2%

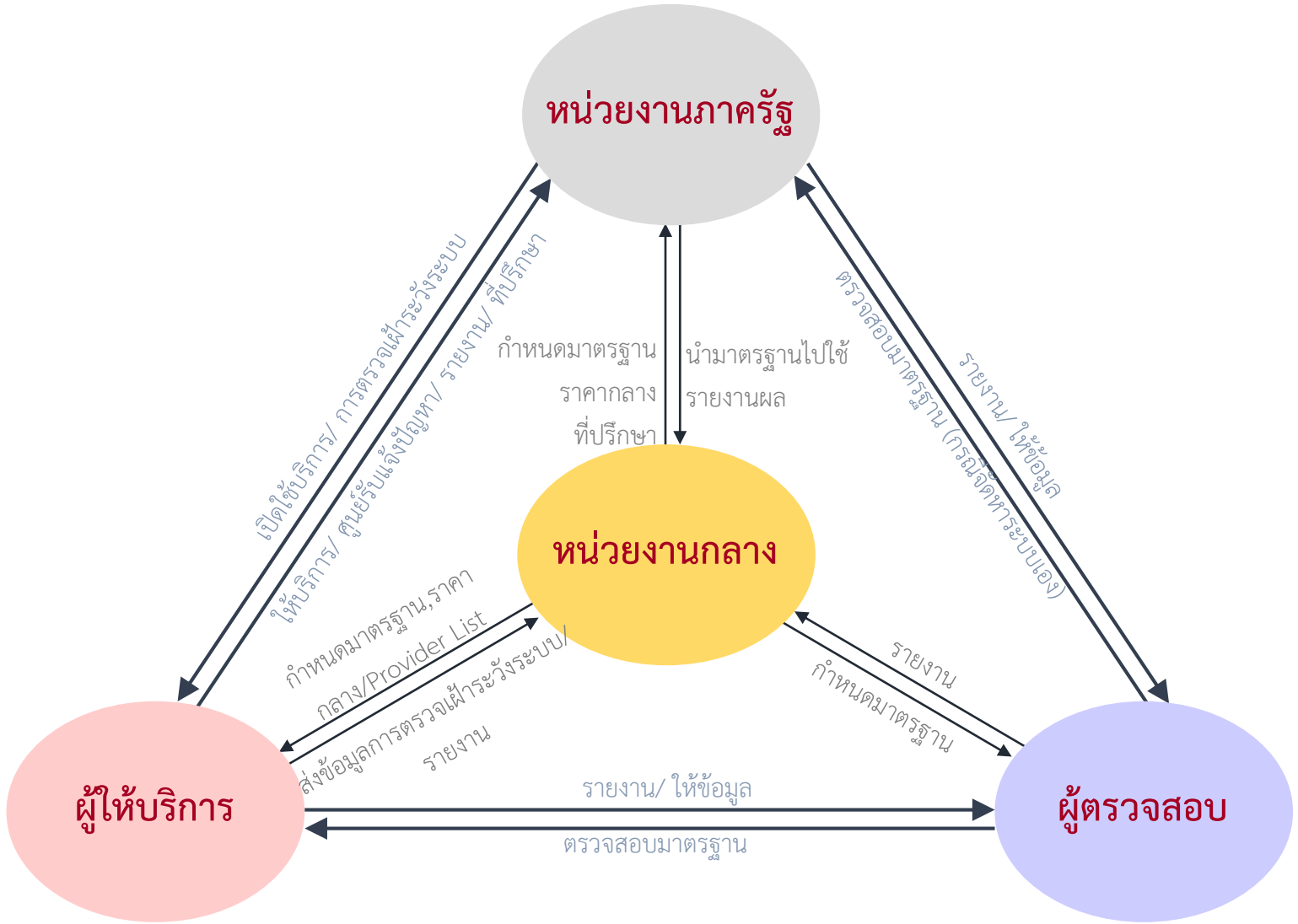


๕. รูปแบบการกำกับดูแลโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย (Government Secure Intranet Governance Model)

รูปแบบการกำกับดูแล โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

แนวคิดในการพัฒนาโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย เป็นการจัดทำมาตรฐานบริการกลาง และแนวทางปฏิบัติในการใช้บริการโครงสร้างพื้นฐานดิจิทัลที่สะดวก พร้อมใช้ ปลอดภัย และน่าเชื่อถือสำหรับหน่วยงานภาครัฐ ซึ่งมี **รูปแบบการกำกับดูแล (GSI Governance Model) โดยกำหนดบทบาทตามหน้าที่รับผิดชอบไว้ ๔ กลุ่ม ดังนี้**

- กลุ่มที่ ๑ **หน่วยงานกลาง**
- กลุ่มที่ ๒ **ผู้ให้บริการ**
- กลุ่มที่ ๓ **หน่วยงานภาครัฐ**
- กลุ่มที่ ๔ **ผู้ตรวจสอบ**



รูปแบบการกำกับดูแล โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

หน่วยงานกลาง มีหน้าที่ดังนี้

๑. จัดทำกรอบแนวทางโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย
๒. จัดทำนโยบาย มาตรฐาน กฎระเบียบ คู่มือ และแนวปฏิบัติ
๓. จัดทำ Government Intranet eXchange (GIX)
๔. กำหนดคุณลักษณะเฉพาะและราคากลาง
๕. กำหนดผู้ตรวจสอบ (GSI Auditor List)
๖. กำหนดผู้ให้บริการ (GSI Provider List)
๗. ประเมิน ตรวจสอบ และติดตามสถานการณ์ แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ
๘. ตรวจสอบรายงานสรุปการใช้บริการในภาพรวมทั้งหมด รวมถึงติดตามประสิทธิภาพการทำงานของผู้ให้บริการ
๙. ให้การสนับสนุน ส่งเสริม และให้คำปรึกษาการดำเนินงาน
๑๐. สร้างความตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

หน่วยงานภาครัฐ มีหน้าที่ดังนี้

๑. ปฏิบัติตามมาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย
๒. ใช้บริการโครงสร้างพื้นฐานดิจิทัลจากผู้ให้บริการที่ผ่านมาตรฐาน
๓. ประเมิน วิเคราะห์ และตรวจสอบปริมาณการใช้งานบริการต่างๆ
๔. จัดตั้งงบประมาณและค่าใช้จ่ายที่เกี่ยวข้อง
๕. จัดทำแผนการใช้ทรัพยากรและแผนการบริหารด้านเทคโนโลยีสารสนเทศ
๖. ตรวจสอบการบริหารจัดการด้านความมั่นคงปลอดภัย และรายงานการใช้บริการจากผู้ให้บริการเพื่อนำมาพัฒนาปรับปรุงคุณภาพให้เกิดประสิทธิภาพมากยิ่งขึ้น
๗. ติดตามสถาณการณ์ แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามที่เกิดขึ้น

รูปแบบการกำกับดูแล โครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย

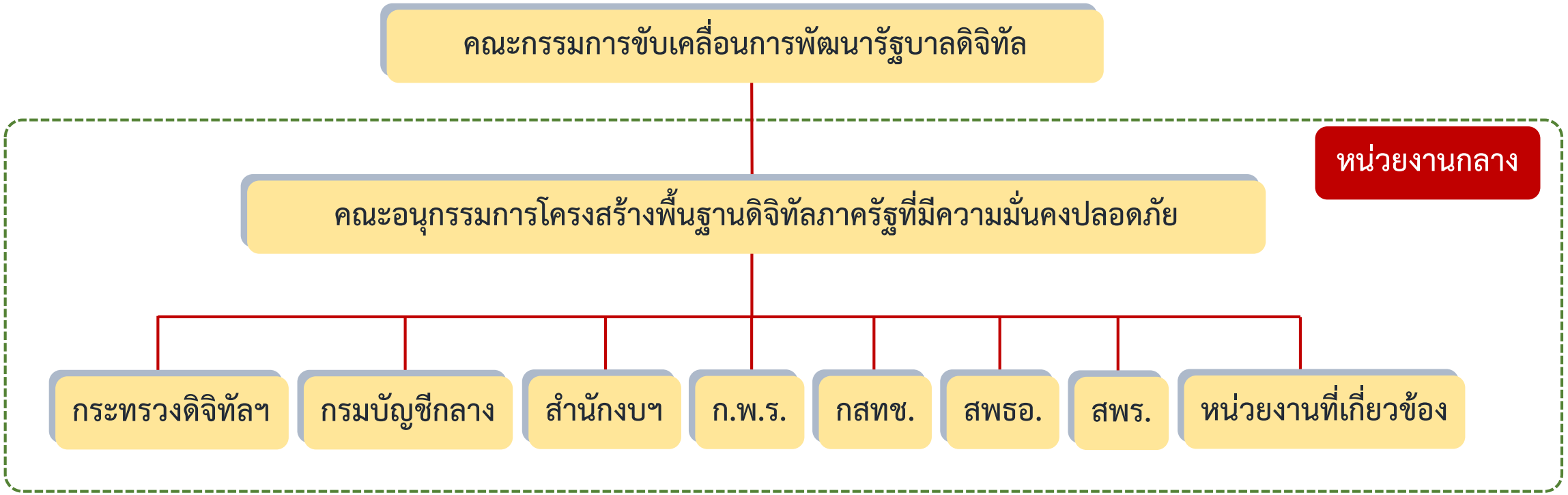
ผู้ให้บริการ มีหน้าที่ดังนี้

๑. ปฏิบัติตามมาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย
๒. มีระบบเฝ้าระวัง (Monitoring) และตรวจสอบ ติดตาม รวมถึงแจ้งเตือนไปยังผู้ที่เกี่ยวข้องในกรณีพบเหตุผิดปกติหรือภัยคุกคาม
๓. มีศูนย์บริการรับแจ้งปัญหาและให้คำปรึกษา วิเคราะห์ ตรวจสอบ แก้ไขเหตุขัดข้อง เมื่อมีเหตุขัดข้องในการให้บริการ
๔. จัดทำรายงานสำหรับหน่วยงานกลาง และหน่วยงานภาครัฐที่ใช้บริการ
๕. จัดทำระบบการคิดค่าบริการแบบอัตโนมัติ
๖. สร้างความตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
๗. ร่วมกำหนดราคากลาง
๘. จัดอบรม (Training) เพื่อสร้างความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

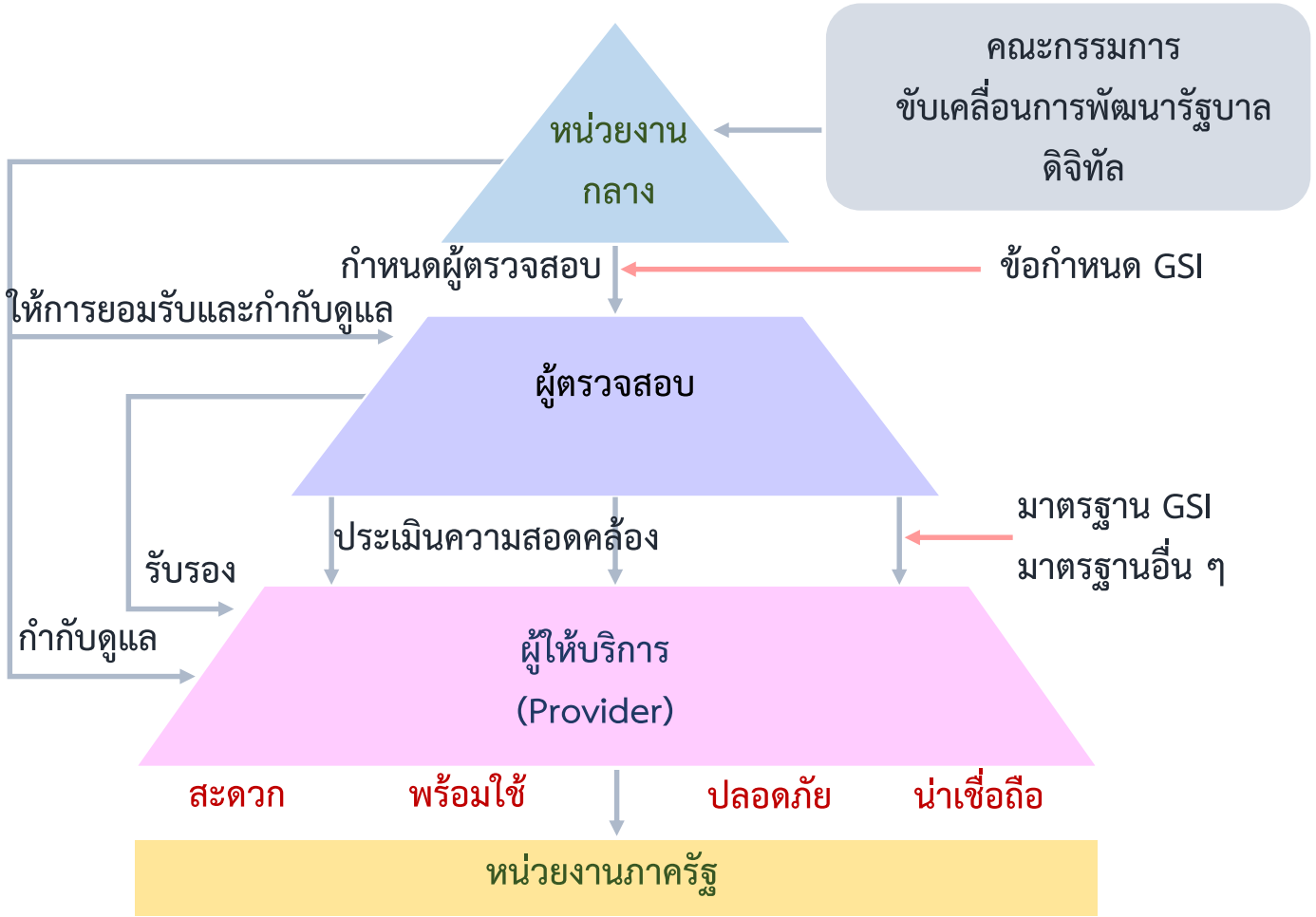
ผู้ตรวจสอบ มีหน้าที่ดังนี้

๑. ตรวจสอบมาตรฐานบริการของผู้ให้บริการ ให้เป็นไปตามมาตรฐานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย
๒. ตรวจสอบหน่วยงานภาครัฐตามมาตรฐานโครงสร้างพื้นฐานดิจิทัลภาครัฐที่มีความมั่นคงปลอดภัย สำหรับหน่วยงานที่ดำเนินการโครงสร้างพื้นฐานดิจิทัลด้วยตนเอง
๓. รายงานผลการตรวจสอบผู้ให้บริการตามมาตรฐานบริการโครงสร้างพื้นฐานดิจิทัลที่มีความมั่นคงปลอดภัย
๔. **รับรองมาตรฐานบริการแก่หน่วยงานภาครัฐที่จัดหาบริการเองและผู้ให้บริการ**

โครงสร้างของ หน่วยงานกลาง



โครงสร้างการตรวจสอบและรับรอง GSI



หน่วยงานกลาง ภายใต้การกำกับดูแลของคณะกรรมการขับเคลื่อนการพัฒนารัฐบาลดิจิทัล ให้การยอมรับ กำหนดผู้ตรวจสอบ และกำกับดูแลหน่วยงานภาครัฐที่จัดหาบริการเอง ผู้ตรวจสอบและผู้ให้บริการตามมาตรฐานและข้อกำหนด GSI

ผู้ตรวจสอบ เป็นหน่วยงานประเภทบุคคลที่สาม (Third Party) ที่ทำหน้าที่ตรวจ รับรอง ประเมินกระบวนการและบริการ ตามมาตรฐาน GSI

THANK YOU