Booklet 2 – Strategy

Thai

[Text to be displayed on the cover]

(ร่าง) แผนยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ

(Draft) Government Data Center Modernization Strategy

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์กรมหาชน) (สรอ.)

Electronic Government Agency (Public Organization) (EGA)

คำนำ

ตลอดหลายปีที่ผ่านมา หลายประเทศพัฒนาและปรับปรุงเทคโนโลยีโครงสร้างพื้นฐานสารสนเทศและการสื่อสารมาอย่างต่อเนื่อง เนื่องจากทั้งการดำเนินงานของภาครัฐ เศรษฐกิจ สังคม และประชาชน ล้วนจำเป็นต้องอาศัยเทคโนโลยีในการปฏิบัติงาน พัฒนาประเทศ และดำรงชีวิตประจำวัน ภาครัฐในหลายประเทศส่วนใหญ่ประสบกับความท้าทายที่คล้ายคลึงกัน เช่น ความต้องการใช้เทคโนโลยีทันสมัย ความต้องการของประชาชนเพื่อเข้าถึงข้อมูลต่างๆ ความสามารถในการจัดการข้อมูลปริมาณมากจากระบบต่างๆ และความจำเป็นในการบูรณาการระบบเทคโนโลยีที่เพิ่มมากขึ้น ซึ่งภาครัฐพยายามหาแนวทางเพื่อขับเคลื่อนประเทศให้ตอบสนองความต้องการในแต่ละด้านได้ นับจากการปฏิวัติอุตสาหกรรมครั้งที่ 4 (The Fourth Industrial Revolution) นั้น ประเทศไทยเป็นหนึ่งในประเทศแนวหน้าของภูมิภาคที่มีการพัฒนาทางเทคโนโลยีเพื่อขับเคลื่อนการเติบโตทางเศรษฐกิจและความเจริญทางสังคม ซึ่งหน่วยงานภาครัฐลงทุนเม็ดเงินมหาศาลเพื่อพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ให้สามารถรองรับการใช้งาน ปริมาณข้อมูลที่ขยายตัว ความต้องการความปลอดภัยสารสนเทศที่เพิ่มมากขึ้น และสอดคล้องกับเทคโนโลยีสมัยใหม่เพื่อนำไปสู่การพัฒนาประเทศอย่างต่อเนื่อง

จากการศึกษาโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) ของประเทศไทยพบว่า ความมั่นคงปลอดภัยสารสนเทศ (ความปลอดภัยสารสนเทศและความสามารถของหน่วยงานในการจัดการข้อมูลสำคัญที่ต้องการความปลอดภัยระดับสูง) การจัดการและการบูรณาการข้อมูล และความล้าสมัยของศูนย์ข้อมูลเป็นประเด็นความท้าทายในอันดับแรกที่หน่วยงานภาครัฐในประเทศไทยกำลังเผชิญอยู่ นอกจากนี้ การบริหารงบประมาณที่ขาดประสิทธิภาพและการขาดความรู้ในการใช้งานโครงสร้างพื้นฐานด้านข้อมูลที่เพียงพอ ล้วนส่งผลให้ค่าใช้จ่ายในการดำเนินงานของศูนย์ข้อมูลนั้นสูงขึ้น นอกจากนี้ การศึกษาโครงการพัฒนาศูนย์ข้อมูลภาครัฐในเชิงลึก ซึ่งผ่านการวิจัย การพูดคุย การประชุมระดมความคิดเห็นกลุ่มย่อย การวิเคราะห์ การจัดทำยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ การจัดทำมาตรฐานบริการศูนย์ข้อมูล และการประชุมรับฟังความคิดเห็น ตลอดระยะเวลา 5 เดือนนั้น ได้เผยคุณลักษณะทั้ง 5 สำหรับทิศทางอนาคตของการพัฒนาศูนย์ข้อมูลภาครัฐสำหรับประเทศไทย คือ 1) การจัดการความปลอดภัยอย่างมีประสิทธิภาพ 2) ความสามารถในการรองรับการขยายตัวของบริการ 3) การออกแบบเพื่อรองรับอนาคต 4) การเพิ่มประสิทธิภาพด้านต้นทุน และ 5) การดำเนินงานอย่างมีประสิทธิภาพ นอกจากนี้ การศึกษาครั้งนี้ระบุรูปแบบการดำเนินงานโครงสร้างพื้นฐานด้านข้อมูลในอนาคตทั้ง 6 รูปแบบซึ่งสำคัญที่สุด คือ 1) Agency Own Data Center, 2) Ministry-Level Data Center, 3) Cross-Agency Data Center, 4) 3rd Party Colocation/Physical Hosting, 5) 3rd Party Services และ 6) G-Services ซึ่งแผนการพัฒนาศูนย์ข้อมูลภาครัฐ นั้นครอบคลุมระยะเวลา 5 ปี ในการดำเนินงานที่ถูกจัดแบ่งเป็นระยะต่างๆ เพื่อพัฒนาโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทย และยังมีการกำหนด 9 โครงการย่อยภายใต้ยุทธศาสตร์การดำเนินงานเพื่อให้ง่ายต่อการบริหารจัดการและดำเนินงานยุทธศาสตร์ GDCM อย่างมีประสิทธิภาพ

จากสิ่งสำคัญต่างๆ ที่กล่าวมาข้างต้น จึงทำให้มั่นใจว่าการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐจะบรรลุเป้าหมาย ผลลัพธ์ และพัฒนาโครงสร้างพื้นฐานด้านข้อมูลของหน่วยงานภาครัฐไทยอย่างสัมฤทธิ์ผล

สารบัญ

1. บทสรุปผู้บริหาร

รัฐบาลในหลายประเทศทั่วโลกมีการดำเนินงานเพื่อบริหารและพัฒนาประเทศของตน เช่น การกำหนดนโยบาย การบริหารจัดการภายในภาครัฐ การให้บริการแก่ภาคธุรกิจและประชาชน เป็นต้น ซึ่งโครงสร้างพื้นฐานด้านข้อมูล (Data Infrastructure) โครงสร้างพื้นฐานกายภาพ (Physical Infrastructure) การทำ Virtualization และระบบคลาวด์ (Cloud System) ล้วนเป็นเทคโนโลยีที่สำคัญต่อการดำเนินงานของภาครัฐอย่างมีประสิทธิภาพ โดยโครงสร้างพื้นฐานด้านข้อมูลของภาครัฐซึ่งเป็นโครงสร้างหลักสำหรับการดำเนินงานนั้นประกอบด้วย ข้อมูลที่เป็นความลับ ข้อมูลสำคัญที่ใช้กำกับการบริการของภาครัฐ และข้อมูลสาธารณะ นอกจากนี้ โครงสร้างพื้นฐานด้านข้อมูลยังสามารถรวมถึงระบบที่ใช้จัดเก็บและบริหารข้อมูล เช่น ศูนย์ข้อมูลภาครัฐและโครงสร้างพื้นฐานของภาคเอกชนอีกด้วย

หน่วยงานภาครัฐหลายแห่งมีการจัดทำยุทธศาสตร์ศูนย์ข้อมูล (Data Center Strategy) เพื่อสนับสนุนดิจิทัลโรดแมป (Digital Roadmap) หรือการขับเคลื่อนการพัฒนาดิจิทัลของประเทศ โดยเริ่มจากการพัฒนาศูนย์ข้อมูลที่มีอยู่เดิมและยกระดับเทคโนโลยีสารสนเทศ (IT) ให้สามารถรองรับความต้องการและสามารถให้บริการอย่างมีประสิทธิภาพ การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization) จึงเป็นการดำเนินงานที่มีความสำคัญเพื่อสนับสนุนโครงสร้างพื้นฐานด้านข้อมูลให้มีความเสถียร ยืดหยุ่น ปลอดภัย คุ้มค่า และยั่งยืน นอกจากนี้ การรักษาความสมดุลระหว่างความต้องการบริการเทคโนโลยีสารสนเทศที่เพิ่มขึ้นกับข้อจำกัดด้านงบประมาณของหน่วยงานภาครัฐยังเป็นอีกเรื่องที่ควรได้รับการดูแลเป็นอย่างยิ่ง

ประเทศไทยกำลังเปลี่ยนแปลงไปสู่การเป็นผู้นำด้านดิจิทัลและมีการพัฒนาภาคส่วนต่างๆ ให้สอดคล้อง ซึ่งภาคส่วนดังกล่าวนั้นรวมถึง โครงสร้างพื้นฐาน การบริการของภาครัฐ ภาคอุตสาหกรรม และภาคธุรกิจ เป็นต้น อย่างไรก็ดี หน่วยงานภาครัฐของไทยยังอาจต้องเผชิญกับความท้าทาย เช่น ความซับซ้อนของระบบเทคโนโลยีสารสนเทศ กระบวนการที่ยังต้องพึ่งพาแรงงานคน การขาดความสามารถในการดูแลระบบเทคโนโลยีสารสนเทศ การขาดงบประมาณและบุคลากรที่เพียงพอ นอกจากนี้ ปริมาณข้อมูลอิเล็กทรอนิกส์ที่เพิ่มขึ้น การใช้ระบบคลาวด์ที่ขยายตัวและมีแนวโน้มสูงขึ้น และความต้องการพื้นที่จัดเก็บข้อมูลที่ปลอดภัยในราคาที่เหมาะสมที่มากขึ้นนั้น ยังเป็นแรงกดดันให้ศูนย์ข้อมูลในประเทศไทยมีความจำเป็นต้องมีการให้บริการที่ทันสมัยเพื่อรองรับความต้องการต่างๆ เหล่านั้น

ทิศทางอนาคตของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทย (Future State for Thailand Government's Data Infrastructure) มีนิยามว่า โครงสร้างพื้นฐานที่ทำขึ้นใหม่จากการพัฒนาองค์ประกอบต่างๆ เช่น วิสัยทัศน์และเป้าหมายของภาครัฐ ยุทธศาสตร์โครงสร้างพื้นฐานด้านข้อมูล โครงสร้างพื้นฐานปัจจุบัน ความคาดหวัง ความต้องการของประชาชนและหน่วยงานภาครัฐ รวมถึงความเสี่ยงและความท้าทายที่ภาครัฐเผชิญในปัจจุบันและในอนาคต โครงสร้างพื้นฐานด้านข้อมูลของไทยจำเป็นต้องมียุทธศาสตร์การพัฒนา (Modernization Strategy) เพื่อสร้างความคล่องตัว ความปลอดภัย ความคุ้มค่า และความมีประสิทธิภาพ ทิศทางอนาคตของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทยภายใต้ชื่อ การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) ประกอบด้วย 5 คุณลักษณะที่โดดเด่นและมีความแตกต่างจากโครงสร้างพื้นฐานเดิมซึ่งจะเป็นรากฐานสำคัญสำหรับยุทธศาสตร์อนาคต ประกอบด้วย 1) การจัดการความปลอดภัยอย่างมีประสิทธิภาพ 2) ความสามารถในการรองรับการขยายตัวของบริการ

3) การออกแบบเพื่อรองรับอนาคต 4) การเพิ่มประสิทธิภาพด้านต้นทุน และ 5) การดำเนินงานอย่างมีประสิทธิภาพ ในอนาคตอันใกล้ โครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทยจะถูกพัฒนาและกำกับดูแลภายใต้แผนยุทธศาสตร์ของการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) อย่างน้อยในระยะ 5 ปี (ปี ค.ศ. 2018 - 2022) โดยมีรูปแบบการดำเนินงานในอนาคตของโครงสร้างพื้นฐานด้านข้อมูลทั้ง 6 รูปแบบ ได้แก่ 1) Agency Own Data Center, 2) Ministry-Level Data Center, 3) Cross-Agency Data Center, 4) 3rd Party Colocation/Physical Hosting Hosting, 5) 3rd Party Services และ 6) G-Services ซึ่งหน่วยงานสามารถเลือกใช้เพื่อเพิ่มประสิทธิภาพและมีความเหมาะสมตามความต้องการของหน่วยงาน โดยพิจารณาจากการดำเนินงานปัจจุบันเป็นที่ตั้ง ซึ่งรูปแบบการดำเนินงานในอนาคตทั้ง 6 นี้ หากปฏิบัติพร้อมกับมาตรฐานบริการศูนย์ข้อมูล (Data Center Service Standards) ที่เหมาะสม จะสามารถเพิ่มประสิทธิภาพการดำเนินงานและการใช้จ่ายงบประมาณได้อย่างมากอีกด้วย

แผนการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ถูกจัดทำขึ้นโดยอาศัยความเข้าใจและการวิเคราะห์โครงสร้างพื้นฐานด้านข้อมูลของประเทศไทย โครงสร้างพื้นฐานทางกายภาพ แอปพลิเคชัน การจัดตั้งศูนย์ข้อมูล ความคิดเห็นของหน่วยงานต่างๆ และวิธีปฏิบัติที่เป็นเลิศ (Best Practice) ในระดับสากล ผลจากการศึกษาทำให้เข้าใจถึงแนวโน้มและความต้องการในการพัฒนาศูนย์ข้อมูลของประเทศไทย ความคาดหวังของหน่วยงาน ปัญหาที่หน่วยงานกำลังเผชิญ และประเด็นที่สำคัญอื่นๆ โดยโครงการพัฒนาศูนย์ข้อมูลภาครัฐนำมาซึ่งประโยชน์ที่สำคัญ ได้แก่ ความมั่นคงปลอดภัยของข้อมูลภาครัฐ บริการที่มีประสิทธิภาพและคุ้มค่า ความรับผิดชอบขึ้นกับหน่วยงานที่เหมาะสม ข้อจำกัดด้านบุคลากรที่ลดลง และเทคโนโลยีโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของไทยที่มีความทันสมัย นอกจากนี้ โครงการพัฒนาศูนย์ข้อมูลภาครัฐยังครอบคลุมการนำมาตรฐานบริการศูนย์ข้อมูลที่สำคัญมาใช้ใน 5 มิติ ได้แก่ 1) Energy and Power, 2) Design and Structure, 3) Server, Storage and Utilization, 4) Location and Site และ 5) Service Level Agreement (SLA) ซึ่งมาตรฐานบริการศูนย์ข้อมูลทั้ง 5 มิตินี้จะยกระดับและเพิ่มประสิทธิภาพการให้บริการ

ในระยะ 5 ปีข้างหน้านี้ หน่วยงานภาครัฐของไทยถูกคาดหวังว่าจะพิจารณาการยกระดับโครงสร้างพื้นฐานด้านข้อมูลและบรรลุตามวัตถุประสงค์ที่วางไว้ของรัฐบาลเป็นที่เรียบร้อย ทั้งนี้ ตัวชี้วัดประสิทธิภาพด้านยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐนั้นสามารถแบ่งออกเป็นด้านต่างๆ ได้แก่ Asset and Capacity Utilization, Human Resources Utilization, Shared Services, Cost Optimization, Security และ Strategic Framework ซึ่งการนำยุทธศาสตร์การพัฒนาศูนย์ข้อมูลมาปฏิบัติจะส่งเสริมความก้าวหน้า ศักยภาพ นวัตกรรม และการดำเนินงานร่วมกันของทุกภาคส่วนในประเทศ

การดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐในระยะ 5 ปีนั้น สามารถแบ่งออกเป็น 3 ระยะ ดังนี้

- ระยะที่ 1 - Readiness ซึ่งครอบคลุมระยะเวลา 1 ปี โดยมุ่งเน้นการเตรียมความพร้อมของภาครัฐและหน่วยงานในการเปลี่ยนแปลง
- ระยะที่ 2 - Adoption ซึ่งครอบคลุมระยะเวลา 2 ปี โดยนำแผนการพัฒนาศูนย์ข้อมูลภาครัฐ มาใช้
- ระยะที่ 3 - Improvement ซึ่งครอบคลุมระยะเวลา 2 ปีนับจากเสร็จสิ้นระยะที่ 2 โดยมุ่งเน้นการติดตามและปรับปรุงการดำเนินงานอย่างต่อเนื่อง

นอกจากนี้ การดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐนั้นถูกบริหารจัดการภายใต้โครงการย่อยทั้งหมด 9 โครงการ ซึ่งสอดคล้องกับการดำเนินงานยุทธศาสตร์ทั้ง 3 ระยะข้างต้นเพื่อให้การดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐนั้นประสบผลสำเร็จ โดยโครงการย่อยทั้ง 9 โครงการนี้ ได้แก่ iDiscover, iTransform, iOptimize, iTransition, iAdopt, iChange, iLearn, iMonitor และ iNegotiate เมื่อดำเนินงานทั้งหมดเสร็จสิ้นสมบูรณ์แล้วจะส่งผลให้โครงสร้างพื้นฐานด้านข้อมูลของประเทศไทย เป็นระบบที่มีประสิทธิภาพ มาตรฐาน คล่องตัว ปลอดภัย คุ้มค่า และรองรับความต้องการในอนาคต

2. ที่มาของโครงการ

ตลอดทศวรรษที่ผ่านมา มีปัจจัยหลายประการที่ส่งผลให้หน่วยงานภาครัฐในหลายประเทศมุ่งเน้นการพัฒนาศูนย์ข้อมูล (Data Center Modernization) โดยทางด้านเทคโนโลยีนั้น ศูนย์ข้อมูลปัจจุบันจำเป็นต้องรองรับความต้องการที่เพิ่มขึ้น ต้องมีความสามารถขยายตัวและยืดหยุ่นในการให้บริการ ต้องรองรับการทำ Virtualization และสามารถรองรับการปฏิบัติงานที่เปลี่ยนแปลงอย่างรวดเร็ว แต่ในมุมมองทางด้านสิ่งแวดล้อมนั้น ศูนย์ข้อมูลเหล่านี้เผชิญแรงกดดันเพื่อให้ใช้พลังงานอย่างเหมาะสมและลดผลกระทบต่อสิ่งแวดล้อม ส่วนด้านเศรษฐกิจศูนย์ข้อมูลมีความจำเป็นต้องเพิ่มผลตอบแทนให้ได้สูงสุดจากระบบต่างๆ ที่มีอยู่ ซึ่งขณะเดียวกันความจำเป็นในการปรับปรุงระบบศูนย์ข้อมูลและกระบวนการด้าน IT เช่น การรักษาเวลาให้บริการ (Uptime) การบูรณาการระบบเทคโนโลยีศูนย์ข้อมูลที่ซับซ้อน และการใช้ทรัพยากรที่มีอยู่ให้เกิดประโยชน์สูงสุด นั้นยิ่งทวีความสำคัญเพิ่มขึ้น

หน่วยงานภาครัฐหลายหน่วยงานได้พัฒนายุทธศาสตร์ศูนย์ข้อมูลเพื่อให้สอดคล้องกับดิจิทัลโรดแมป (Digital Roadmap) หรือทิศทางการพัฒนาดิจิทัลของประเทศ หน่วยงานเหล่านี้เริ่มจากการพัฒนาศูนย์ข้อมูลของตนที่มีอยู่ แล้วดำเนินการพัฒนาปรับปรุงระบบ IT ให้มีประสิทธิภาพสูงสุด ถึงแม้วัตถุประสงค์หลักของการพัฒนาศูนย์ข้อมูลนั้นมีความหลากหลาย แต่การเพิ่มความเสถียร ความปลอดภัยของศูนย์ข้อมูล และ ประสิทธิภาพของการปฏิบัติงานและการใช้งบประมาณนั้นยังเป็นวัตถุประสงค์หลักที่ช่วยผลักดันดิจิทัลโรดแมป (Digital Roadmap) หรือทิศทางการพัฒนาดิจิทัลของประเทศ

การพัฒนาศูนย์ข้อมูลเกิดขึ้นทั่วโลกเพราะมีความสำคัญต่อภาครัฐ ซึ่งความต้องการใช้จ่ายงบประมาณให้ได้ประโยชน์สูงสุดและตอบสนองต่อความต้องการที่จะให้บริการแก่ประชาชนอย่างมีประสิทธิภาพมากที่สุดคือเหตุผลสำคัญของการพัฒนาศูนย์ข้อมูล โดยมีตัวอย่างประเทศที่ได้มีการดำเนินการดังต่อไปนี้

สาธารณรัฐเกาหลี: เกาหลีใต้ถือเป็นประเทศแรกๆ ที่ตระหนักถึงความสำคัญของการพัฒนาศูนย์ข้อมูลภาครัฐ โดยเกาหลีใต้ก่อตั้งหน่วยงานภาครัฐเพื่อดำเนินการพัฒนาศูนย์ข้อมูลกลางสำหรับหน่วยงานต่างๆ จำนวน 2 แห่ง ในระหว่างปี ค.ศ. 2005 - 2007 และดำเนินการควบรวมศูนย์ข้อมูลภาครัฐอย่างต่อเนื่องจนถึงปี ค.ศ. 2011

สหรัฐอเมริกา: สหรัฐอเมริกาเริ่มดำเนินการควบรวมศูนย์ข้อมูลในปี ค.ศ. 2010 ภายใต้โครงการ Federal Data Center Consolidation Initiative (FDCCI) โดยโครงการดังกล่าวได้รับการประเมินว่าสามารถลดค่าใช้จ่ายได้มากกว่า 2 พันล้านเหรียญสหรัฐจากการควบรวมศูนย์ข้อมูลในช่วงระหว่างปี ค.ศ. 2010 - 2015 หลังจากนั้น รัฐบาลสหรัฐอเมริกาได้ดำเนินโครงการ Data Center Optimization Initiative (DCOI) แทนที่โครงการ FDCCI ในปี ค.ศ. 2016

สหราชอาณาจักร: รัฐบาลสหราชอาณาจักรดำเนินโครงการควบรวมระบบจัดเก็บข้อมูล และเทคโนโลยีศูนย์ข้อมูลที่กระจัดกระจายกันอยู่ให้เป็นระบบบริหารจัดการแบบรวมศูนย์ โครงการนี้ช่วยให้รัฐบาลสหราชอาณาจักรประหยัดค่าใช้จ่ายได้มากถึง 105 ล้านปอนด์

เครือรัฐออสเตรเลีย: รัฐบาลออสเตรเลียประมาณการว่าสามารถลดค่าใช้จ่ายถึง 1 พันล้านเหรียญสหรัฐด้วยการบูรณาการศูนย์ข้อมูลทั้งหมดเข้าด้วยกัน ซึ่งโครงการดังกล่าวขยายเวลาดำเนินงานไปจนถึงปี ค.ศ. 2025 โดยระยะที่ 1 ของแผนควบรวมศูนย์ข้อมูลประกอบด้วยการรวบรวมความต้องการพื้นที่ศูนย์ข้อมูลและการนิยามมาตรฐานที่ใช้ในการจัดซื้ออุปกรณ์และพื้นที่

ศูนย์ข้อมูล ระยะที่ 2 คือการใช้วิธีการและเทคโนโลยีร่วมกันระหว่างหน่วยงาน และระยะที่ 3 คือการนำเทคโนโลยี กระบวนการ และนโยบายใหม่ๆ มาใช้ให้เกิดประโยชน์

สาธารณรัฐสิงคโปร์: รัฐบาลสิงคโปร์เป็นผู้ใช้บริการ Private Cloud มาตั้งแต่ปี ค.ศ. 2012 และใช้บริการโครงสร้างพื้นฐานทั้งหมดจากผู้ให้บริการศูนย์ข้อมูลภายนอก โดยมี Singapore Telecommunications Limited (Singtel) เป็นผู้ให้บริการ

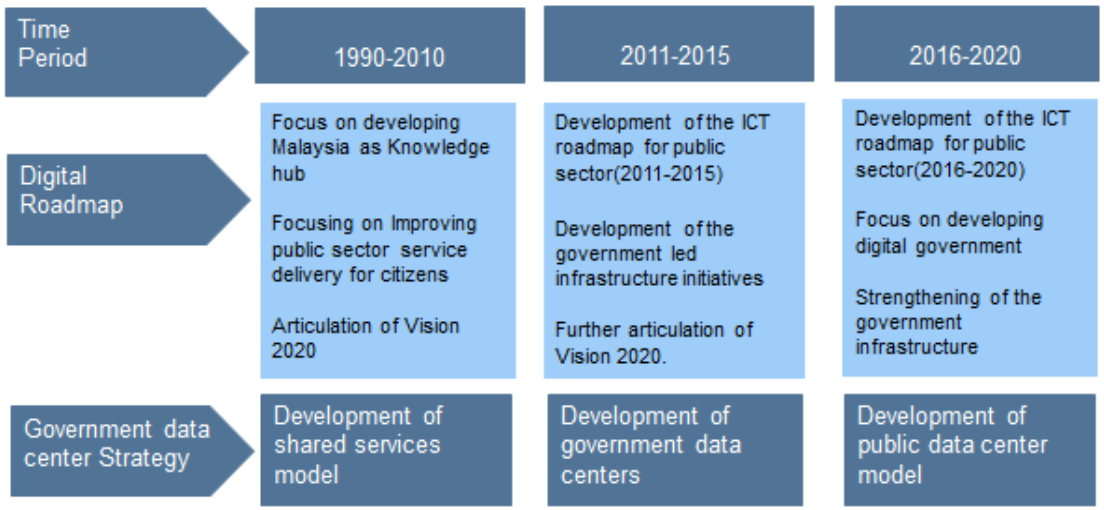
ประเทศแคนาดา: โครงการ Shared Services Center (SSC) ในแคนาดาเป็นการบูรณาการศูนย์ข้อมูลภาครัฐทั้ง 485 แห่ง ให้เหลือเพียง 7 แห่ง ซึ่งสิ่งอำนวยความสะดวกที่ทันสมัยจะได้รับการออกแบบให้สามารถรองรับความต้องการของประชาชนและภาครัฐ รวมถึงการรองรับเทคโนโลยีที่เปลี่ยนแปลงอยู่ตลอดเวลา การควบรวมศูนย์ข้อมูลภาครัฐนี้ยังสามารถลดผลกระทบต่อสิ่งแวดล้อม โดยการลดขนาดศูนย์ข้อมูลจาก 600,000 ตารางฟุตเป็น 180,000 ตารางฟุต และจากเครื่องแม่ข่าย 23,000 เครื่องเป็น 14,000 เครื่องเท่านั้น จึงทำให้สามารถลดการใช้พลังงานได้เป็นจำนวนมาก

เขตบริหารพิเศษฮ่องกงแห่งสาธารณรัฐประชาชนจีน: รัฐบาลฮ่องกงตระหนักถึงความสำคัญของศูนย์ข้อมูลและมูลค่าของเศรษฐกิจที่ศูนย์ข้อมูลสามารถขับเคลื่อนให้แก่ประเทศ ฮ่องกงได้พัฒนาพื้นที่เศรษฐกิจที่มีความเหมาะสมในการเปิดบริการศูนย์ข้อมูลขึ้นหลายแห่ง อีกทั้งรัฐบาลยังได้เริ่มการพัฒนาพิมพ์เขียว (Blueprint) เพื่อการควบรวมศูนย์ข้อมูลด้วย

สหพันธรัฐมาเลเซีย: ประเทศมาเลเซียวางแผนเปลี่ยนระบบการทำงานของภาครัฐให้กลายเป็นระบบดิจิทัลทั้งหมดภายในปี ค.ศ. 2020 โดยเริ่มดำเนินการควบรวมศูนย์ข้อมูลในปี ค.ศ. 2011 ตามแผนเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับปี ค.ศ. 2011 - 2015 หลังจากนั้นรัฐบาลได้เปิดศูนย์ข้อมูลกลางภาครัฐ 2 แห่งในปี ค.ศ. 2015 และหลายหน่วยงานได้เริ่มใช้บริการศูนย์ข้อมูลจากศูนย์ข้อมูลใหม่เหล่านี้ ทั้งนี้ รัฐบาลมาเลเซียคาดหวังว่าหน่วยงานทั้งหมดจะใช้บริการจากศูนย์ข้อมูลกลางภาครัฐภายในปี ค.ศ. 2020

3. เปรียบเทียบกรณีศึกษาการพัฒนาศูนย์ข้อมูลของต่างประเทศ

กรณีศึกษาการพัฒนาศูนย์ข้อมูลภาครัฐของสหพันธรัฐมาเลเซีย

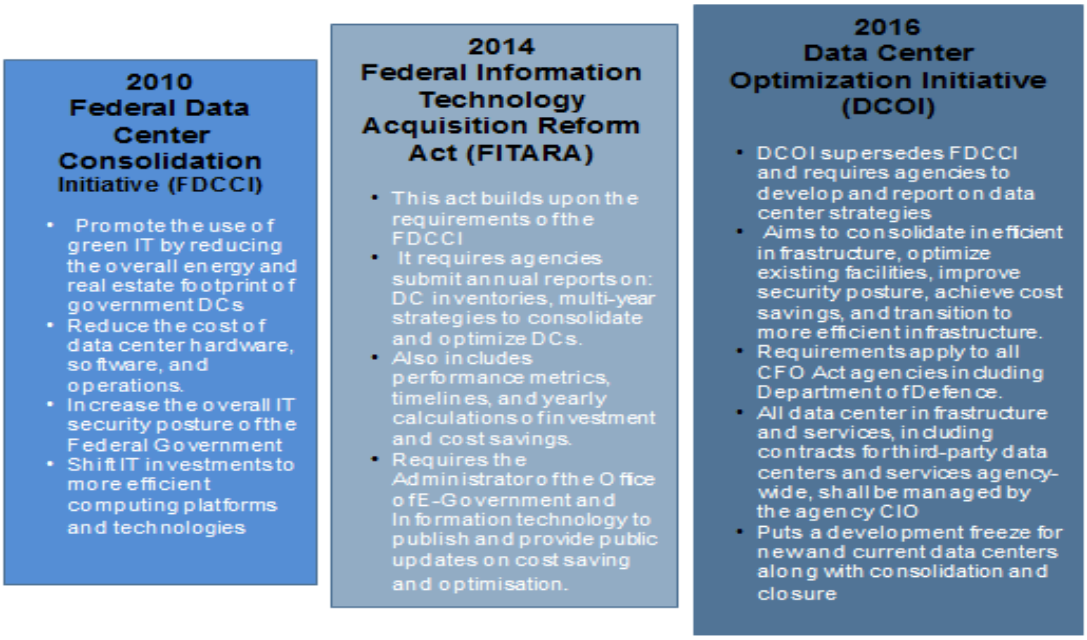


ในช่วงคริสต์ทศวรรษที่ 1990 รัฐบาลมาเลเซียเล็งเห็นว่าการมุ่งเน้นอุตสาหกรรมความรู้ (Knowledge-Based Industry) นั้นเป็นหนทางเพื่อยกระดับประเทศไปสู่การเป็นประเทศรายได้สูง (High-Income Country) การให้ความสำคัญกับเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) และการสร้างองค์ความรู้เพื่อการเติบโตที่ยั่งยืนได้ถูกกล่าวถึงเป็นครั้งแรกในแผนเศรษฐกิจมาเลเซียฉบับที่ 7 (The Seventh Malaysian Economic Plan 1996–2000) โดยในช่วงปี ค.ศ. 2011 - 2015 รัฐบาลมาเลเซียมุ่งเน้นจัดทำโรดแมป (Roadmap) การพัฒนาโครงสร้างพื้นฐานกลางและเครือข่ายสำหรับภาครัฐ และในช่วงปี ค.ศ. 2016 - 2020 รัฐบาลมาเลเซียวางแผนการปรับใช้เทคโนโลยีให้สอดคล้องกับการดำเนินงานของภาครัฐ ปรับกระบวนการด้าน ICT ให้เหมาะสม และมุ่งเน้นความคุ้มค่าสูงสุดจากการลงทุนโดยใช้ประโยชน์จากเทคโนโลยีและการดำเนินงานด้าน ICT ที่วางแผนมาเป็นอย่างดี

ในช่วงปี ค.ศ. 2011 - 2015 รัฐบาลมาเลเซียได้จัดตั้งเครือข่ายภาครัฐ 1Gov*net ขึ้นมาโดยมีหน่วยงานภาครัฐเริ่มใช้งานมากกว่า 20 แห่ง นอกจากนี้ ในช่วงเดียวกันรัฐบาลมาเลเซียให้ความสำคัญกับกระบวนการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization) และได้ผนวกการพัฒนาศูนย์ข้อมูลภาครัฐไว้ในแผนงาน ICT ปี ค.ศ. 2011 - 2015 ซึ่งรัฐบาลมาเลเซียจัดตั้งศูนย์ข้อมูลกลางจำนวน 2 แห่ง โดยมีหน่วยงานภาครัฐจำนวน 84 หน่วยงานใช้ศูนย์ข้อมูลกลาง Government Data Center 1 (GDC1) และมีหน่วยงานจำนวน 50 หน่วยงานที่ใช้งาน Government Data Center 2 (GDC2) นอกจากนี้ รัฐบาลมาเลเซียยังเริ่มใช้บริการระบบสื่อสารแบบครบวงจร (Unified Communication Services) ที่หน่วยงานกลาง Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) ได้จัดหา โดยมีผู้ใช้งานกว่า 284,027 ราย และภายในปี ค.ศ. 2020 รัฐบาลมาเลเซียวางแผนที่จะจัดตั้งศูนย์ข้อมูลกลางอีก 6 แห่ง และวางแผนให้หน่วยงานภาครัฐของตนย้ายไปใช้เครือข่ายภาครัฐทั้งหมด พร้อมทั้งให้หน่วยงานมากกว่า 90% ย้ายไปจัดเก็บข้อมูลบนระบบคลาวด์อีกด้วย

กรณีศึกษาการพัฒนาศูนย์ข้อมูลภาครัฐของสหรัฐอเมริกา

หน่วยงาน Office of E-Government and Information Technology (E-Gov) ที่มี Chief Information Officer (CIO) ของรัฐบาลกลาง (Federal Government) เป็นผู้บริหารสูงสุดได้จัดทำแผนควบรวมศูนย์ข้อมูลรัฐบาลกลางขึ้นมาในปี ค.ศ. 2010 นอกเหนือจากนี้ หน่วยงาน E-Gov ยังอยู่ภายใต้หน่วยงาน Office of Management and Budget (OMB) ซึ่งเป็นหน่วยงานที่มีขนาดใหญ่ที่สุดภายใต้สำนักประธานาธิบดีแห่งสหรัฐอเมริกา (Executive Office of the President of the United States) อีกด้วย



รัฐบาลสหรัฐอเมริกาเปิดตัวโครงการ Federal Data Center Consolidation Initiative (FDCCI) เพื่อส่งเสริมการใช้เทคโนโลยีสารสนเทศประหยัดพลังงาน (Green IT) โดยมีแนวทางปฏิบัติเพื่อลดการใช้พลังงานโดยรวม ลดผลกระทบจากศูนย์ข้อมูล และลดค่าใช้จ่ายด้านต่างๆ ของศูนย์ข้อมูล เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และการดำเนินงาน โดยที่มีการยกระดับความปลอดภัยด้าน IT ของรัฐบาลกลางควบคู่กันไป

จนถึงปัจจุบัน ศูนย์ข้อมูลภาครัฐที่หน่วยงานเป็นผู้ดำเนินการเองได้ปิดการให้บริการไปแล้วกว่า 4,300 แห่งจากทั้งหมดประมาณ 11,000 แห่งและส่งผลให้ภาครัฐสามารถประหยัดค่าใช้จ่ายได้ถึง 2,800 ล้านเหรียญสหรัฐจนถึงปีงบประมาณ ค.ศ. 2015 นอกจากนี้ รัฐบาลสหรัฐอเมริกายังคาดการณ์จะสามารถประหยัดค่าใช้จ่ายได้อีกอย่างน้อย 5 พันล้านเหรียญสหรัฐหรือมากกว่านั้นอีกด้วย

โครงการ Data Center Optimization Initiative (DCOI) ซึ่งเป็นโครงการล่าสุดที่ถูกดำเนินการต่อจากโครงการ FDCCI นั้นกำหนดให้หน่วยงานต่างๆ ต้องปฏิบัติตามเงื่อนไขภายในปี ค.ศ. 2018 ดังต่อไปนี้

- หน่วยงานต้องติดตั้งมิเตอร์อัจฉริยะเพื่อวัดการใช้พลังงานและต้องรายงานการใช้พลังงานอย่างครบถ้วนให้แก่ Office of Management and Budget ซึ่งเป็นหน่วยงานของรัฐบาลทราบ
- ศูนย์ข้อมูลที่มีอยู่เดิมต้องดำเนินงานโดยมีประสิทธิภาพการใช้พลังงาน (PUE) ที่ 1.5 หรือต่ำกว่า ภายในระยะเวลาที่กำหนด มิเช่นนั้นอาจถูกปิดตัวลงหากเลยกำหนดระยะเวลา

- ไม่อนุญาตให้หน่วยงานรายงานผลการใช้พลังงานแบบ Manual และหน่วยงานต้องใช้เครื่องมือ Data Center Infrastructure Management (DCIM) เพื่อติดตามสถานการณ์ทำงานของศูนย์ข้อมูลแบบอัตโนมัติ

4. แนวทางเชิงยุทธศาสตร์

การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization)

การพัฒนาศูนย์ข้อมูล (Data Center Modernization) มีวัตถุประสงค์เพื่อพัฒนาขีดความสามารถของภาครัฐในการบริหารจัดการข้อมูลเพื่อให้บรรลุเป้าหมายต่างๆ ที่กำหนดไว้ของประเทศโดยอาศัยโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ดี

หลายประเทศทั่วโลกมีโครงสร้างศูนย์ข้อมูลที่มีประสิทธิภาพเพื่อรองรับกลไกภาครัฐให้ดำเนินงานอย่างราบรื่น ในยุคเศรษฐกิจดิจิทัลปัจจุบัน รัฐบาลและหน่วยงานภาครัฐเร่งใช้ประโยชน์จากแอปพลิเคชันและการให้บริการเทคโนโลยีสารสนเทศเพื่อให้ทันสมัยอยู่เสมอ ทั้งนี้โครงสร้างพื้นฐานด้านข้อมูลที่มีประสิทธิภาพจะมีความพร้อมและสามารถรองรับการประมวลผลได้เป็นอย่างดีเพื่อช่วยให้หน่วยงานมีความก้าวหน้าในด้านเทคโนโลยีและการให้บริการ เทคโนโลยีสำคัญที่ขับเคลื่อนการพัฒนาศูนย์ข้อมูลนั้นประกอบด้วย Cloud Computing, Flash Storage, Virtualization และ Software-Defined Network ซึ่งแผนกเทคโนโลยีสารสนเทศของหน่วยงานกำลังเผชิญแรงกดดันที่มากขึ้นเพื่อให้เพิ่มคุณค่าให้แก่หน่วยงาน นอกจากการปฏิบัติงานตามภารกิจแล้ว แผนกเทคโนโลยีสารสนเทศยังถูกคาดหวังในการให้แนะนำและดำเนินการใช้งานเทคโนโลยีใหม่ๆ ในหน่วยงาน เช่น การทำ Server Virtualization, Cloud Computing และ Software-Defined Infrastructure เป็นต้น ฉะนั้นการพัฒนาศูนย์ข้อมูลจะเป็นตัวแปรสำคัญที่เพิ่มคุณค่าให้หน่วยงานและเป็นปัจจัยสำคัญช่วยให้ผู้บริหารมีข้อมูลสำหรับการตัดสินใจเพื่อเพิ่มศักยภาพในการดำเนินงานได้ดียิ่งขึ้น เนื่องจากการพัฒนาศูนย์ข้อมูลจะเพิ่มประสิทธิภาพ เพิ่มความปลอดภัย ยกระดับการเชื่อมต่อ ยกระดับการจัดเก็บข้อมูล เพิ่มประสิทธิภาพซอฟต์แวร์ และประหยัดค่าใช้จ่ายการดำเนินงาน เป็นต้น ภาครัฐในหลายประเทศให้ความสำคัญกับการพัฒนาด้านเทคโนโลยีสารสนเทศผ่านประโยชน์จากการพัฒนาโครงสร้างพื้นฐานที่มีประสิทธิภาพและความปลอดภัย

คำนิยาม

การพัฒนาศูนย์ข้อมูล (Data Center Modernization) คือการตัดสินใจในระดับองค์กรเพื่อปรับโครงสร้างการรวบรวมและจัดเก็บข้อมูลบนพื้นฐานความต้องการขององค์กร รวมถึงการพิจารณาแนวโน้มทางเศรษฐกิจและเทคโนโลยีใหม่ที่มีให้เลือกใช้

การพัฒนาศูนย์ข้อมูลภาครัฐ: แนวทางทั่วโลกในภาพรวม (Government Data Center Modernization: Global Approach)

ปัจจุบันนี้หน่วยงานภาครัฐหลายแห่งยังไม่สามารถบริหารความสมดุลระหว่างความต้องการบริการทางเทคโนโลยีที่เพิ่มขึ้นและข้อจำกัดด้านงบประมาณได้ดีเท่าที่ควร รวมถึงความซับซ้อนและต้องการด้านข้อมูลที่เพิ่มขึ้น นอกจากนี้ การบำรุงรักษาระบบเทคโนโลยีสารสนเทศแบบดั้งเดิม (Legacy IT System) เริ่มลดลงเนื่องจากการดูแลระบบฮาร์ดแวร์และซอฟต์แวร์ที่ล้าสมัยนั้นมีค่าใช้จ่ายสูงและขาดความปลอดภัย

นอกจากนี้ หน่วยงานภาครัฐยังเผชิญกับความท้าทายอื่นๆ โดยตลอด เช่น ความซับซ้อนของระบบ IT กระบวนการทำงานที่ยังต้องอาศัยเจ้าหน้าที่ (Manual Process) ความสามารถในการดูแลระบบ การขาดแคลนบุคลากร และงบประมาณ

ที่เพียงพอ ซึ่งความท้าทายเหล่านี้มีความเชื่อมโยงกับระบบ IT ที่ล้าสมัยโดยตรง ส่งผลให้หน่วยงานไม่สามารถสร้างสรรค์บริการใหม่ ไม่สามารถให้บริการประชาชนอย่างมีประสิทธิภาพ และไม่มีความปลอดภัยสารสนเทศ การใช้ระบบดั้งเดิมมักมีความซ้ำซ้อนและสิ้นเปลืองทรัพยากรที่มีอยู่อย่างจำกัด ซึ่งเพิ่มความซับซ้อนให้แก่หน่วยงานในการบริหารจัดการขึ้นอีก ซึ่งหลายหน่วยงานในปัจจุบันกำลังหยุดใช้ระบบแบบดั้งเดิมและเริ่มใช้ระบบที่ทันสมัยมากขึ้น

5. ประเทศไทย – แผนเทคโนโลยีสารสนเทศและการสื่อสาร

ทุกวันนี้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) มีส่วนสำคัญในชีวิตประจำวันมากขึ้นและยังเป็นปัจจัยสำคัญในการขับเคลื่อนการเติบโตทางเศรษฐกิจ สร้างเสถียรภาพทางสังคม และพัฒนาประเทศอย่างยั่งยืน ประเทศไทยกำลังเดินหน้าเปลี่ยนแปลงตนเองเพื่อเป็นผู้นำด้านดิจิทัล แนวโน้มทางดิจิทัลใหม่ๆ เช่น Big Data, Internet of Things, Social Media, Mobile Advertising และ Cloud Computing ล้วนเป็นตัวเร่งการเปลี่ยนแปลงวิถีที่ผู้คนปฏิสัมพันธ์กันและยังเปลี่ยนแปลงสภาพแวดล้อมทางธุรกิจโดยสิ้นเชิง ที่สำคัญ รัฐบาลไทยมุ่งเน้นวิสัยทัศน์ Digital Thailand เพื่อยกระดับความสามารถในการแข่งขันของอุตสาหกรรมต่างๆ ในประเทศและคาดหวังให้ประเทศไทยเป็นผู้นำด้านดิจิทัลในภูมิภาคอาเซียน

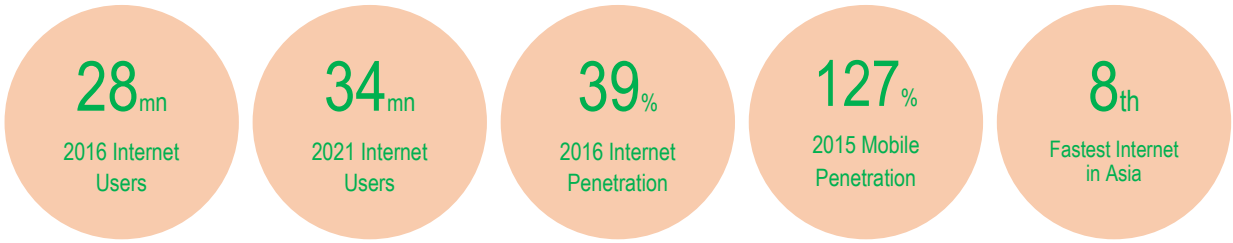
Digital Thailand คือ ประเทศไทยในรูปแบบใหม่ที่เพิ่มการใช้ประโยชน์เทคโนโลยีดิจิทัลในทุกกิจกรรมทางสังคมและเศรษฐกิจเพื่อพัฒนาโครงสร้างพื้นฐาน ข้อมูล นวัตกรรม ทรัพยากรบุคคล และทรัพยากรดิจิทัลอื่นๆ เพื่อขับเคลื่อนประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน

จากผลการสำรวจ The United Nations E-Government Survey ปี ค.ศ. 2016 นั้น ประเทศไทยอยู่ในอันดับที่ 77 จากทั้งหมด 193 ประเทศและเขตการปกครอง ในดัชนีพัฒนาการด้านรัฐบาลอิเล็กทรอนิกส์ (E-Government Development Index) ซึ่งประเทศไทยนั้นพัฒนาขึ้นมาถึง 25 อันดับจากปี ค.ศ. 2014 และเป็นอันดับที่ 4 ในภูมิภาคอาเซียน

ค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ทั้งหมดของประเทศไทยมีมูลค่าเพิ่มขึ้นประมาณ 21 พันล้านเหรียญสหรัฐฯ ในปี ค.ศ. 2015 ซึ่งคิดเป็น 7% ของผลผลิตมวลรวมภายในประเทศ (GDP)

การขยายตัวของอุตสาหกรรม ICT ได้รับแรงกระตุ้นจากแผนพัฒนาเศรษฐกิจดิจิทัลของรัฐบาล อีกทั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในขณะนั้น) ยังได้วางแผนจัดตั้งอินเทอร์เน็ตเกตเวย์ในระดับภูมิภาค (Regional Internet Gateway) ด้วยการเพิ่มสายเคเบิ้ลใต้น้ำเพื่อรองรับการใช้งานอินเทอร์เน็ตที่เพิ่มขึ้นและเพื่อเป็นศูนย์กลางการเชื่อมต่ออินเทอร์เน็ตในภูมิภาคอาเซียนภายในปี ค.ศ. 2020 นอกจากนี้ ประเทศไทยยังลงทุนติดตั้งสายเคเบิ้ลใต้น้ำเพื่อเชื่อมต่อจากประเทศอินเดียมายังประเทศไทยเพื่อผ่านไปยังประเทศฮ่องกงซึ่งจะสามารถดึงดูดปริมาณข้อมูลทางอินเทอร์เน็ตให้เพิ่มขึ้นจาก “อนุภูมิภาคลุ่มแม่น้ำโขง” (Great Mekong Subregion) ซึ่งมีประชากรกว่า 270 ล้านคนในปัจจุบัน รัฐบาลได้กำหนดแผนการนำเทคโนโลยีดิจิทัลมาใช้ในการพัฒนาเศรษฐกิจและสังคม นอกจากนั้น การปฏิรูปสู่เศรษฐกิจดิจิทัลถือเป็นก้าวสำคัญในการพัฒนาเศรษฐกิจของประเทศเนื่องจากนำเทคโนโลยี ICT มาบริหารจัดการธุรกิจและการบริการต่างๆ อีกทั้งการปฏิรูปสู่เศรษฐกิจดิจิทัลส่งผลให้รัฐบาลปรับปรุงแนวทางการให้บริการและการทำธุรกรรมผ่านทางอิเล็กทรอนิกส์อีกด้วย

ในปี ค.ศ. 2015 ประเทศไทยมีผู้ใช้งานสมาร์ทโฟนประมาณ 40 ล้านคน โดยคาดว่าการใช้งานสมาร์ทโฟนจะเพิ่มขึ้นเป็นอีกเท่าตัวภายในปี ค.ศ. 2021 ที่สำคัญ แนวโน้มการใช้งานสมาร์ทโฟนที่เพิ่มขึ้นจะกระตุ้นการขยายตัวของอินเทอร์เน็ตบรอดแบนด์ไร้สาย (Mobile Broadband) ในประเทศไทย นอกจากนั้น อัตราการใช้งานสมาร์ทโฟนจะเพิ่มขึ้นเป็น 60% ของอัตราการใช้โทรศัพท์เคลื่อนที่ทั้งหมดในปี ค.ศ. 2016 และคาดการณ์ว่าจะเพิ่มสูงขึ้นจนถึง 80% ภายในปี ค.ศ. 2021



***แหล่งที่มา**: Stastica, Worldbank, Bangkokpost, NBTC*

ในปี ค.ศ. 2015 ประเทศไทยและประเทศสิงคโปร์เป็นเพียง 2 ประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่มีอัตราลงทะเบียนใช้งานบรอดแบนด์ไร้สาย (Mobile Broadband Subscription) เกินกว่า 100% ซึ่งอัตราลงทะเบียนใช้งานบรอดแบนด์ไร้สายในไทยเพิ่มขึ้นไปถึง 120% ในปี ค.ศ. 2015 และถูกคาดว่าอาจเพิ่มถึง 160% ภายในปี ค.ศ. 2021 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในขณะนั้น) ได้จัดทำทิศทางการพัฒนาดิจิทัลของประเทศขึ้น โดยมีเป้าหมายเพื่อพัฒนาประเทศไปสู่ Digital Thailand อย่างเต็มรูปแบบในอีก 20 ปีข้างหน้า

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

เป้าหมายของรัฐบาลในการพัฒนาเศรษฐกิจและสังคมดิจิทัลสำหรับประเทศไทยนั้นเป็นหนึ่งในโครงการระยะสั้นและระยะกลางที่มีความสำคัญต่อการกำหนดทิศทางอนาคตของประเทศ ที่สำคัญ การผลักดัน Digital Thailand นั้นมีประโยชน์โดยตรงต่อการเติบโตของผลผลิตมวลรวมภายในประเทศ ความเจริญรุ่งเรือง สังคม เศรษฐกิจ อัตราการจ้างงาน ผลิตภาพแรงงาน และความสามารถในการแข่งขันในระดับนานาชาติ นอกจากนี้ แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมยังกำหนดยุทธศาสตร์ระยะยาวในการพัฒนาโครงสร้างพื้นฐาน แรงงาน และทรัพยากรอื่นๆ เพื่อรองรับความต้องการของภาคประชาชนและธุรกิจที่เปลี่ยนแปลงอย่างรวดเร็ว และเพื่อขับเคลื่อนนวัตกรรมดิจิทัลและสร้างโอกาสใหม่ๆ

รัฐบาลวางแผนการร่วมมือกับภาคเอกชนเพื่อพัฒนาโครงสร้างพื้นฐานทางกายภาพ (Hard Infrastructure) ของประเทศไทยให้มีศักยภาพรองรับเศรษฐกิจดิจิทัล ทั้งนี้ แผน Digital Thailand ยังสร้างโอกาสให้แก่ภาคธุรกิจอื่นๆ เช่น บริษัทเปิดใหม่ (Start-up) และวิสาหกิจขนาดกลางและขนาดย่อม (SME) ทั้งนี้ ภาคธุรกิจดังกล่าวจะได้รับการส่งเสริมจากศูนย์ฝึกอบรมและโครงการแบ่งปันองค์ความรู้ด้าน E-Commerce ซึ่งในอนาคต ธุรกิจ E-Commerce และธุรกิจด้านการขนส่ง (Logistic) จะได้รับประโยชน์จากการเติบโตอย่างรวดเร็วของตลาด E-Commerce

แผนพัฒนารัฐบาลดิจิทัลของประเทศไทยปี พ.ศ. 2560 - 2564

แผนพัฒนารัฐบาลดิจิทัลของประเทศไทยปี พ.ศ. 2560 - 2564 เน้นการพัฒนาขีดความสามารถด้านดิจิทัลในทุกภาคส่วน เช่น การเกษตร การท่องเที่ยว การศึกษา การสาธารณสุข การลงทุน และการป้องกันภัยธรรมชาติ เป็นต้น เพื่อขับเคลื่อนความก้าวหน้าทางเศรษฐกิจและสังคม ซึ่งอาจบรรลุผลได้ต่อเมื่อมีการนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้ในการให้บริการแก่ประชาชน

แผนพัฒนารัฐบาลดิจิทัลของประเทศไทยประกอบด้วย 5 ยุทธศาสตร์ดังนี้

1. การยกระดับคุณภาพชีวิตประชาชน
2. การยกระดับขีดความสามารถการแข่งขันของภาคธุรกิจ
3. การยกระดับความมั่นคงและเพิ่มความปลอดภัยของประชาชน
4. การยกระดับประสิทธิภาพภาครัฐ
5. การบูรณาการและยกระดับโครงสร้างพื้นฐานรัฐบาลดิจิทัล

วิสัยทัศน์ของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยคือ “เพื่อผลักดันภาครัฐของประเทศไทยสู่การเป็นรัฐบาลดิจิทัลที่มีการบูรณาการระหว่างหน่วยงาน มีการปฏิบัติงานเชิงสร้างสรรค์ มีการให้บริการโดยให้ประชาชนเป็นศูนย์กลาง และมีการขับเคลื่อนการเปลี่ยนแปลงอย่างแท้จริง”

ภายใต้ยุทธศาสตร์ที่ 4 ของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยนั้นมีเป้าหมายหลักคือ การบูรณาการและการยกระดับประสิทธิภาพการดำเนินงานภาครัฐผ่านการเชื่อมโยงระบบจากหลายหน่วยงานเพื่อเพิ่มขีดความสามารถเชิงดิจิทัลภาครัฐในการบริหารจัดการการเงินและการใช้จ่าย การจัดซื้อจัดจ้าง การบริหารสินทรัพย์ และทรัพยากรมนุษย์ เพื่อยกระดับการดำเนินงานภาครัฐให้สะดวก รวดเร็ว โปร่งใส และสนับสนุนการพัฒนาสู่รัฐบาลดิจิทัลโดยสมบูรณ์

ภายใต้ยุทธศาสตร์ที่ 5 ของแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยนั้นมีเป้าหมายหลักคือ การบูรณาการการให้บริการภาครัฐผ่านการเชื่อมโยงระบบจากหลายหน่วยงานและการพัฒนาโครงสร้างพื้นฐานการให้บริการอิเล็กทรอนิกส์ของภาครัฐ ซึ่งปฏิบัติควบคู่กับการยกระดับขีดความสามารถและทักษะเชิงดิจิทัลให้กับเจ้าหน้าที่ภาครัฐในทุกระดับและทุกหน่วยงานเพื่อเป็นรากฐานของการพัฒนาหน่วยงานภาครัฐให้เป็นรัฐบาลดิจิทัลโดยสมบูรณ์

ทั้งนี้ การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ถือเป็นเสาหลักในการขับเคลื่อนยุทธศาสตร์ที่ 4 และ 5 ในการยกระดับประสิทธิภาพภาครัฐและบูรณาการโครงสร้างพื้นฐานรัฐบาลดิจิทัล นอกจากนี้ การพัฒนาศูนย์ข้อมูลภาครัฐยังส่งเสริมการใช้ประโยชน์จากโครงสร้างพื้นฐานและทรัพยากรภาครัฐ เพิ่มประสิทธิภาพโครงสร้างพื้นฐานด้านข้อมูล พัฒนาโครงสร้างพื้นฐานเพื่อรองรับความต้องการในอนาคต และเสริมสร้างโครงสร้างพื้นฐานรัฐบาลดิจิทัลให้มีความยั่งยืน

เมืองอัจฉริยะของประเทศไทย (Thailand Smart Cities)

รัฐบาลจัดสรรงบประมาณ 97 ล้านบาทเพื่อยกระดับจังหวัดภูเก็ตให้เป็นเมืองอัจฉริยะภายใต้โครงการ Smart Thailand ซึ่งโครงการดังกล่าวมีเป้าหมายเพื่อให้ประเทศไทยเปลี่ยนแปลงสู่การเป็นศูนย์กลางดิจิทัลของภูมิภาคอาเซียน การพัฒนาเมืองอัจฉริยะของประเทศไทยถือเป็นส่วนสำคัญโดยเป็นส่วนหนึ่งของนโยบายพัฒนาเศรษฐกิจดิจิทัลของรัฐบาล จังหวัดภูเก็ตได้ก้าวไปสู่การเป็น “เมืองอัจฉริยะ” ในปี ค.ศ. 2016 ส่วนจังหวัดเชียงใหม่มีแผนเพื่อเปลี่ยนแปลงสู่การเป็น “เมืองอัจฉริยะ” ในปี ค.ศ. 2017 ซึ่งการเป็นเมืองอัจฉริยะนั้นสามารถดึงดูดบริษัทเปิดใหม่ (Start-up) ด้านเทคโนโลยีและการลงทุนด้านดิจิทัล กระตุ้นอุตสาหกรรมท่องเที่ยว และยกระดับคุณภาพชีวิตประชาชน ที่สำคัญ รัฐบาลวางเป้าหมายที่จะพัฒนาเมืองอัจฉริยะทั่วประเทศโดยเปิดโอกาสให้จังหวัดต่างๆ สามารถพัฒนาเมืองอัจฉริยะตามความเหมาะสมทางเศรษฐกิจและสังคมของแต่ละจังหวัด

6. ประเทศไทย – ภาพรวมของกระทรวงและหน่วยงานต่างๆ

โครงสร้างการบริหารงานของรัฐบาลไทยประกอบด้วยกระทรวง ทบวง และกรม ในแต่ละกระทรวงมีรัฐมนตรีผู้เป็นสมาชิกของคณะรัฐมนตรีเป็นผู้บริหารสูงสุด โดยทบวงอาจเป็นหน่วยงานอิสระที่มีฐานะเทียบเท่ากระทรวงหรือสังกัดกระทรวง กระทรวงจะมีการแบ่งภาระหน้าที่รับผิดชอบออกเป็นกรมต่างๆ โดยมีอธิบดีทำหน้าที่เป็นหัวหน้าหน่วยงาน นอกจากนี้ โครงสร้างการบริหารงานของรัฐบาลยังมีหน่วยงานส่วนกลางคือ สำนักนายกรัฐมนตรี ซึ่งมีนายกรัฐมนตรีเป็นผู้บริหารสูงสุด ทั้งนี้สำนักนายกรัฐมนตรีนั้นมีฐานะเทียบเท่าหน่วยงานในระดับกระทรวง

นอกจากนี้ ยังมีหน่วยงานอิสระที่อยู่นอกเหนืออำนาจหน้าที่ของกระทรวง ทบวง และกรม โดยเป็นหน่วยงานอิสระที่ตั้งขึ้นตามภารกิจเฉพาะหรือตามกฎหมาย เช่น

- สำนักพระราชวัง
- สำนักราชเลขาธิการ
- สำนักงานคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ
- สำนักงานพระพุทธศาสนาแห่งชาติ
- สำนักงานคณะกรรมการวิจัยแห่งชาติ
- ราชบัณฑิตยสภา
- ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

คณะรัฐมนตรีของไทยประกอบด้วยฝ่ายบริหารของรัฐบาล ซึ่งมีรัฐมนตรีว่าการเป็นผู้บริหารสูงสุดในแต่ละกระทรวง และมีรัฐมนตรีช่วยว่าการเป็นผู้บริหารในลำดับรองลงมา โครงสร้างปัจจุบันของรัฐบาลไทยยังคงรูปแบบเดิมนับตั้งแต่พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545

คณะรัฐมนตรีประกอบด้วยรัฐมนตรีจาก 19 กระทรวง และรัฐมนตรีประจำสำนักนายกรัฐมนตรี นอกจากนี้ กระทรวงต่างๆ สำนักนายกรัฐมนตรี หน่วยงานที่สังกัดกระทรวง และหน่วยงานอิสระอื่นๆ ถือเป็นโครงสร้างบริหารที่ขับเคลื่อนกลไกการดำเนินงานของรัฐบาลไทย

สำนักนายกรัฐมนตรี	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	กระทรวงการคลัง	กระทรวงพาณิชย์
กระทรวงอุตสาหกรรม	กระทรวงเกษตรและสหกรณ์	กระทรวงกลาโหม	กระทรวงคมนาคม
กระทรวงพลังงาน	กระทรวงมหาดไทย	กระทรวงการท่องเที่ยวและกีฬา	กระทรวงการต่างประเทศ
กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	กระทรวงวิทยาศาสตร์และเทคโนโลยี	กระทรวงยุติธรรม	กระทรวงสาธารณสุข
กระทรวงวัฒนธรรม	กระทรวงศึกษาธิการ	กระทรวงแรงงาน	กระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์

7. ประเด็นและความท้าทายสำคัญ

ความต้องการที่มีต่อศูนย์ข้อมูลนั้นเพิ่มมากขึ้นในประเทศไทย เนื่องจากปัจจัยที่สำคัญต่างๆ เช่น การเพิ่มขึ้นของปริมาณข้อมูลอิเล็กทรอนิกส์ การเพิ่มขึ้นของการใช้ระบบคลาวด์ในภาครัฐและธุรกิจ และการเพิ่มขึ้นของความต้องการพื้นที่จัดเก็บข้อมูลที่ปลอดภัยและมีราคาเหมาะสม ในอดีตนั้น การจัดการศูนย์ข้อมูลสามารถดำเนินการได้ง่าย เนื่องจากปัจจัยสำคัญต่างๆ ที่กล่าวมาข้างต้นนั้นยังไม่มีความซับซ้อนมากจนเกินไป แต่เนื่องจากในปัจจุบันนี้ ปริมาณข้อมูลอิเล็กทรอนิกส์นั้นมีแนวโน้มที่จะเพิ่มมากขึ้นอย่างรวดเร็ว ดังนั้น การเตรียมความพร้อมและการบริหารศูนย์ข้อมูลจึงมีความซับซ้อนมากขึ้นไปด้วย เช่น การบูรณาการข้อมูล การจัดการคุณภาพข้อมูล การใช้ประโยชน์ทรัพยากร IT การใช้พลังงานไฟฟ้าและระบบทำความเย็น การจัดการพื้นที่ตู้แร็ค การใช้ประโยชน์พื้นที่จัดเก็บข้อมูล และการนำมาตรฐานศูนย์ข้อมูลมาประยุกต์ใช้ เป็นต้น ซึ่งหน่วยงานต่างๆ จำเป็นต้องวางแผนอย่างรอบคอบในการปฏิบัติงานและใช้จ่ายงบประมาณ

โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) มีจัดการประชุมระดมความคิดเห็นกลุ่มย่อยโดยมีหน่วยงานภาครัฐและเอกชนเข้าร่วมกว่า 42 หน่วยงาน จากการวิเคราะห์ข้อมูลและสรุปผลการประชุมดังกล่าวนั้นแสดงให้เห็นความท้าทายสำคัญ 5 อันดับแรก ที่หน่วยงานภาครัฐไทยกำลังเผชิญในการปฏิบัติงานศูนย์ข้อมูลดังนี้

ความท้าทายของหน่วยงานภาครัฐในประเทศไทย

ในปัจจุบันแผนกเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ของหน่วยงานต่างๆ เผชิญปัญหาด้านการจัดเก็บข้อมูล ปัญหาด้านฮาร์ดแวร์ และการให้บริการแก่ผู้ใช้งาน (End-User) ที่ต้องดำเนินการอย่างมีประสิทธิภาพและคุ้มค่า

แผนภาพและการวิเคราะห์ด้านล่างเป็นการรวบรวมความท้าทายสำคัญที่หน่วยงานภาครัฐไทยกำลังเผชิญ ซึ่งมี 6 มิติหลัก ได้แก่

- **การรักษาความปลอดภัย** ประกอบด้วยการรักษาความปลอดภัยข้อมูล การรักษาความปลอดภัยกายภาพของศูนย์ข้อมูล การจัดการข้อมูลที่สำคัญต่อพันธกิจ (Mission Critical Data)
- **การจัดการข้อมูล** ประกอบด้วยการบูรณาการ การจำแนกประเภทข้อมูล หน่วยงานผู้รับผิดชอบข้อมูล การทำความสะอาดข้อมูล (Data Cleansing) ความถูกต้อง และคุณภาพของข้อมูล
- **ทรัพยากรมนุษย์** ประกอบด้วยการขาดแคลนบุคลากร การขาดแคลนทักษะของบุคลากร และการมีบุคลากรที่มีทักษะไม่เพียงพอ
- **การจัดตั้งศูนย์ข้อมูล** ประกอบด้วยเครื่องแม่ข่าย ระบบจัดเก็บข้อมูล การเดินสายสัญญาณ การติดตั้งระบบทำความเย็นและระบบไฟฟ้า โครงสร้างพื้นอาคาร (Floor Architecture) ตู้แร็ค และการออกแบบอาคาร เป็นต้น
- **งบประมาณและต้นทุน** ประกอบด้วยงบประมาณที่จัดสรรสำหรับค่าใช้จ่าย ต้นทุนการดำเนินงานที่สูงขึ้น และการอัพเกรดระบบ
- **นโยบายและการจัดการของหน่วยงาน** ประกอบด้วยการใช้งานร่วมกัน การวางแผน การใช้งานศูนย์ข้อมูลสำรอง การสำรองข้อมูล และการให้ประชาชนเป็นศูนย์กลางในการดำเนินงาน เป็นต้น

การรักษาความปลอดภัย

- การจัดการความปลอดภัยข้อมูล การรักษาแนวปฏิบัติด้านการรักษาความปลอดภัย และความมั่นใจที่มีต่อการจัดการข้อมูลที่สำคัญต่อพันธกิจ (Mission Critical Data) ได้อย่างมีประสิทธิภาพ คือหนึ่งในหลายๆ ความท้าทายสำคัญที่สุดที่หน่วยงานเผชิญร่วมกัน
- 30% ของหน่วยงานระบุว่าการรักษาความปลอดภัยทางกายภาพของศูนย์ข้อมูลเป็นความท้าทายสำคัญที่กำลังเผชิญอยู่
- หน่วยงานต่างๆ ระบุว่าแรงกดดันในการจัดการความปลอดภัยนั้นมีมากขึ้นตามปริมาณข้อมูลที่เพิ่มขึ้น ซึ่งส่งผลให้ประสบปัญหาการรักษาสมดุลระหว่างระดับการรักษาความปลอดภัยกับปริมาณข้อมูล นอกจากนี้ การโจมตีระบบและความเสี่ยงจากการจัดการข้อมูลชั้นความลับที่เพิ่มขึ้นนั้น ส่งผลให้การจัดการความปลอดภัยกลายเป็นความท้าทายที่เพิ่มขึ้นด้วย

การจัดการข้อมูล

- 54% ของหน่วยงานยอมรับว่า การจัดการข้อมูลเป็นความท้าทายสำคัญประการหนึ่ง
- หน่วยงานกล่าวถึงหลายประเด็นสำคัญในด้านการจัดการข้อมูล เช่น การบูรณาการข้อมูลระหว่างหน่วยงาน ความไม่สอดคล้องของหน่วยงานเจ้าของข้อมูล ความกระจัดกระจายของฐานข้อมูล การทำความสะอาดข้อมูล (Data Cleansing) ข้อมูลไม่อยู่ในรูปแบบอิเล็กทรอนิกส์ การจำแนกประเภทข้อมูลขาดความเหมาะสม ความถูกต้องและความสมบูรณ์ของข้อมูล เป็นต้น

ทรัพยากรมนุษย์

- 28% ของหน่วยงานระบุว่า ปัญหาทรัพยากรมนุษย์เป็นความท้าทายสำคัญ และเป็นอุปสรรคต่อการปฏิบัติงาน
- หน่วยงานระบุว่า บุคลากรด้านศูนย์ข้อมูลมีจำกัดและไม่เพียงพอ โดยเฉพาะอย่างยิ่งบุคลากรที่มีทักษะซึ่งได้รับเข้าบรรจุมานานหลายปีไม่สามารถปรับตัวได้ทันต่อการให้บริการตามความต้องการข้อมูลและโครงสร้างพื้นฐานในปัจจุบันที่ขยายตัวอย่างรวดเร็ว
- เนื่องด้วยงบประมาณที่มีจำกัดและการจัดการโครงสร้างบุคลากร จึงส่งผลให้การเพิ่มจำนวนบุคลากรทำได้ยากและเป็นการสร้างภาระเพิ่มเติมให้แก่บุคลากรด้าน IT ที่มีอยู่เดิม
- การขาดแคลนบุคลากรที่มีทักษะในตลาดแรงงานส่งผลให้ภาครัฐไม่สามารถสรรหาบุคลากรที่มีทักษะมาดำเนินงานได้อย่างเพียงพอ
- หลายหน่วยงานระบุว่าบุคลากรมีจำกัดเนื่องจากข้อจำกัดโครงสร้างบุคลากรและบุคลากรด้าน IT มีแนวโน้มในการเปลี่ยนงานบ่อย นอกจากนี้ ค่าตอบแทนของภาครัฐไม่สามารถดึงดูดบุคลากรที่มีทักษะได้หากเทียบกับภาคเอกชน

การจัดตั้งศูนย์ข้อมูล

- 26% ของหน่วยงานระบุว่า องค์ประกอบของศูนย์ข้อมูล เช่น เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล และอุปกรณ์อื่นๆ ของโครงสร้างพื้นฐานเป็นการสร้างภาระให้แก่หน่วยงาน
- ความท้าทายสำคัญที่สุดในการจัดตั้งศูนย์ข้อมูลคือ การประยุกต์ใช้มาตรฐาน และการเพิ่มประสิทธิภาพศูนย์ข้อมูลไปสู่ระดับเทคโนโลยีที่สูงกว่า
- การประยุกต์ใช้มาตรฐานที่ขาดความสอดคล้องกันระหว่างหน่วยงานหรือกระทรวงทำให้เกิดอุปสรรคในการดำเนินงานร่วมกันภายหลัง
- ความท้าทายอื่นๆ ในการจัดตั้งศูนย์ข้อมูลประกอบด้วย 1) ระบบ IT ที่ใช้งานมานานต้องรับการดูแลเพิ่มขึ้น ส่งผลค่าใช้จ่ายในการดำเนินงานนั้นสูงขึ้น 2) ความต้องการที่เพิ่มขึ้นของขนาดพื้นที่จัดเก็บข้อมูลและเครื่องแม่ข่าย 3) ปัญหาการเดินสายไฟ ระบบทำความเย็น และสถาปัตยกรรมที่ไม่เหมาะสม 4) พื้นที่ไม่เพียงพอ และ 5) ปัญหาการโยกย้ายข้อมูล เป็นต้น

งบประมาณและต้นทุน

- 18% ของหน่วยงานระบุว่า งบประมาณและต้นทุนเป็นความท้าทายสำคัญ
- งบประมาณภาครัฐที่มีจำกัดสวนทางกับความต้องการทรัพยากรด้าน IT ที่เพิ่มขึ้น จึงก่อให้เกิดปัญหาการรักษาคุณภาพและระดับการให้บริการ
- ต้นทุนเพิ่มขึ้นเนื่องจากปัญหาบุคลากร ค่าไฟฟ้า การรักษาความปลอดภัย การฝึกอบรม การจัดการปริมาณข้อมูลจำนวนมาก ความต้องการของผู้ใช้งาน การใช้ทรัพยากร IT อย่างสิ้นเปลือง และอัตราการใช้ประโยชน์จากทรัพยากร IT ในต่ำลง ซึ่งปัจจัยเหล่านี้ก่อให้เกิดอุปสรรคในการดำเนินงานอย่างมีประสิทธิภาพ

นโยบายและการจัดการของหน่วยงาน

- 25% ของหน่วยงานระบุว่า นโยบายและการจัดการในระดับหน่วยงานนั้น มีบทบาทสำคัญในการจัดการศูนย์ข้อมูลอย่างมีประสิทธิภาพ
- หน่วยงานระบุว่า การสำรองข้อมูล (Backup) และการใช้งานศูนย์ข้อมูลสำรอง (Disaster Recovery) ขาดประสิทธิภาพ และการไม่ใช้ทรัพยากรร่วมกันนั้น ส่งผลให้อัตราการใช้ประโยชน์ทรัพยากรนั้นลดลง
- ปริมาณข้อมูลที่มีจำนวนมากขึ้นและการขาดการวางแผนที่ดีนั้น ส่งผลให้หน่วยงานให้บริการแก่ประชาชนและผู้ใช้งานโดยขาดประสิทธิภาพ
- ปัญหาเครือข่าย อาคารที่ต้องปรับปรุง และโครงสร้างพื้นฐานที่ล้าสมัยคือ ความท้าทายอื่นๆ ที่หน่วยงานระบุ

8. สถานะปัจจุบันของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐในประเทศไทย

โครงสร้างพื้นฐานปัจจุบัน

จากการประชุมระดมความคิดเห็นกลุ่มย่อยโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) นั้น หน่วยงานที่เข้าร่วมการประชุมดังกล่าวตระหนักถึงความสำคัญของการพัฒนาและปรับปรุงการดำเนินงานของศูนย์ข้อมูลภาครัฐ โดยได้แสดงความต้องการเพื่อให้มีการเปลี่ยนแปลงที่ดีขึ้น นอกจากนี้ หลายหน่วยงานระบุถึงความจำเป็นของแผนงานระดับชาติที่ต้องจัดทำในการผลักดันให้ทุกหน่วยงานภาครัฐใช้โครงสร้างพื้นฐานร่วมกันเพื่อยกระดับการให้บริการ ประสิทธิภาพ องค์ความรู้ และความเป็นเลิศในการปฏิบัติงาน (Best Practice) อย่างเป็นรูปธรรม

ผลการสำรวจความคิดเห็นของหน่วยงานที่เข้าร่วมการประชุมระดมความคิดเห็นกลุ่มย่อยนั้นสรุปได้ว่า ประเทศไทยจำเป็นต้องมีการพัฒนาการให้บริการศูนย์ข้อมูลใน 4 มิติที่สำคัญที่สุด ดังต่อไปนี้

โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ

ทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT) ประกอบด้วยเครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล อุปกรณ์ต่อพ่วง และซอฟต์แวร์ เป็นต้น ซึ่งทรัพยากรเหล่านี้เป็นองค์ประกอบสำคัญและมีราคาสูง ทรัพยากร IT ยังสามารถครอบคลุมถึงโครงสร้างพื้นฐานด้านเครือข่ายซึ่งอาจมีมูลค่าถึง 65% ของค่าใช้จ่ายโครงสร้างพื้นฐาน (CAPEX) (ไม่นับรวมค่าใช้จ่ายในการลงทุนด้านอสังหาริมทรัพย์) ดังนั้นหน่วยงานภาครัฐจึงควรใช้ประโยชน์จากการลงทุนในทรัพยากร IT เหล่านี้ให้มากที่สุดเพื่อให้การปฏิบัติงานมีประสิทธิภาพ ด้วยเหตุนี้ หน่วยงานต่างๆ จึงจำเป็นต้องผลักดันยุทธศาสตร์เพื่อเปลี่ยนแปลงโครงสร้างพื้นฐานที่ขาดประสิทธิภาพให้มีการใช้งานได้อย่างมีประสิทธิภาพมากขึ้น นอกจากนี้ หน่วยงานต้องยกระดับการจัดการความปลอดภัยและประหยัดต้นทุน ซึ่งหนึ่งในแนวทางที่สามารถทำให้บรรลุวัตถุประสงค์ดังกล่าวคือ การเปลี่ยนไปใช้โครงสร้างพื้นฐานที่มีประสิทธิภาพสูงขึ้น เช่น การใช้บริการคลาวด์ (Cloud) และการใช้บริการร่วมกันระหว่างหน่วยงาน (Shared Services) ซึ่งอำนวยความสะดวกให้หน่วยงานสามารถพัฒนาแอปพลิเคชันใหม่ ดูแล ปรับปรุง และโยกย้ายแอปพลิเคชันได้ง่ายขึ้น โดยอาจพิจารณาถึงต้นทุน และความยืดหยุ่นในการพัฒนาและการให้บริการ

ข้อมูลจากการศึกษาที่ผ่านมาระบุว่าศูนย์ข้อมูลของหน่วยงานภาครัฐในประเทศไทยนั้นมีอัตราการใช้ประโยชน์ที่ต่ำและจำนวน 51% ของหน่วยงานนั้นระบุว่าหน่วยงานของตนไม่ได้ใช้ประโยชน์จากโครงสร้างพื้นฐานอย่างเต็มประสิทธิภาพ

สาเหตุที่นำไปสู่อัตราการใช้ประโยชน์โครงสร้างพื้นฐาน IT ที่ต่ำมีดังต่อไปนี้

บุคลากรด้าน IT ไม่สามารถใช้งานโครงสร้างพื้นฐานได้อย่างเต็มประสิทธิภาพ

งบประมาณจำกัด เนื่องจากต้องนำไปใช้จ่ายในการดำเนินงานและการซ่อมบำรุง

แอปพลิเคชันและข้อมูลที่มีอยู่ไม่ถูกใช้งานอย่างมีประสิทธิภาพ ตลอดจนขาดระบบและขั้นตอนการประเมินการใช้งาน

ขาดการวางแผนเพื่อรองรับความต้องการในอนาคต

ขาดการวางแผนการจัดซื้อที่มีประสิทธิภาพ เนื่องจากไม่มีการศึกษาความเป็นไปได้ (Feasibility) เสียก่อน

ใช้งบประมาณที่ได้รับจากงบประมาณคงเหลือ

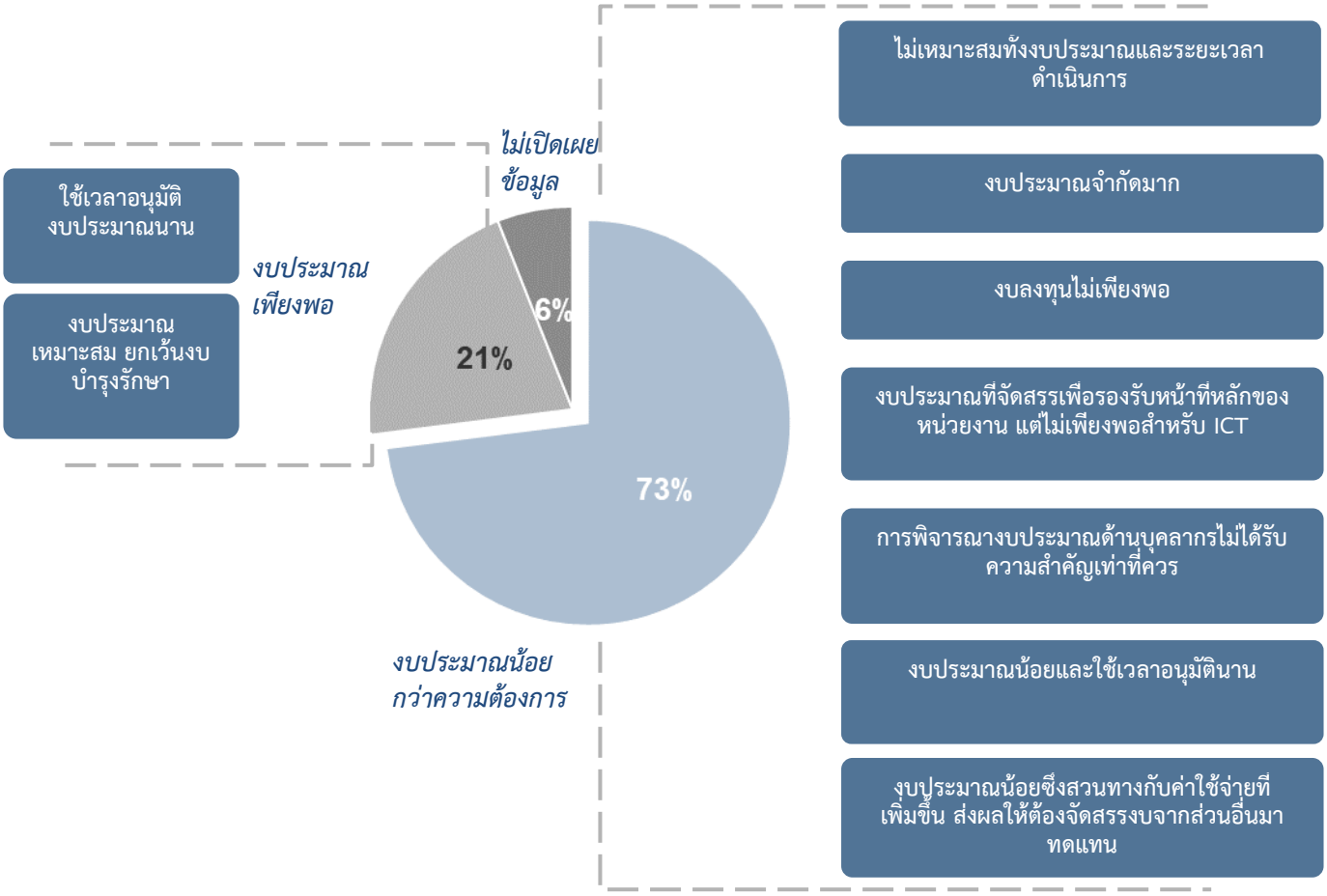
อุปกรณ์มีอายุการใช้งานที่สั้นลง

ประเด็นสำคัญ

- ปัจจุบันหลายหน่วยงานดำเนินงานโดยมีอัตราการใช้ประโยชน์จากทรัพยากร IT ที่ต่ำ เนื่องจากสาเหตุต่างๆ เช่น ขาดการวางแผนที่ดี ขาดการประเมิน ขาดการฝึกอบรม รวมถึงแอปพลิเคชันและข้อมูลไม่ได้ถูกใช้งานอย่างมีประสิทธิภาพ เป็นต้น
- ควรมีการจัดสรรงบประมาณเพื่อพัฒนาโครงสร้างพื้นฐานที่ทันสมัยให้แก่หน่วยงานภาครัฐ เพื่อให้มีโครงสร้างพื้นฐานที่พร้อมใช้งานแก่ทุกหน่วยงานตามความต้องการ และสามารถจัดสรรค่าใช้จ่ายในการดำเนินงานได้อย่างเพียงพอ
- ประเด็นสำคัญของรูปแบบการดำเนินงานในอนาคต (Future Operating Model) คือขั้นตอนการยกระดับอัตราการใช้ประโยชน์ศูนย์ข้อมูล การใช้โครงสร้างพื้นฐานร่วมกันระหว่างหน่วยงาน การใช้โมเดลต่างๆ ในการจัดเก็บข้อมูล และการปรับปรุงอัตราการใช้ประโยชน์ในระดับหน่วยงาน
- อัตราการใช้ประโยชน์จากทรัพยากร IT ที่สูงขึ้นตามมาตรฐานนั้นส่งผลให้ประหยัดค่าใช้จ่าย จัดสรรทรัพยากรได้อย่างเหมาะสม และสามารถวางแผนเพื่อรองรับความต้องการในอนาคตได้ดีขึ้น

งบประมาณ

หน่วยงานที่เข้าร่วมการประชุมระดมความคิดเห็นกลุ่มย่อยโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ระบุว่า ความไม่พร้อมของงบประมาณภาครัฐเป็นอุปสรรคสำคัญต่อการดำเนินงานของหน่วยงาน ขณะเดียวกันในต่างประเทศมีการดำเนินการควบรวมการดำเนินงานศูนย์ข้อมูลเพื่อรับมือกับงบประมาณภาครัฐที่ลดลง ซึ่งงบประมาณที่ลดลงนั้นส่งผลกระทบต่อการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ดังนั้นจึงจำเป็นที่ภาครัฐของประเทศไทยต้องพิจารณาทบทวนเพื่อให้เกิดการดำเนินงานอย่างมีประสิทธิภาพ



ประเด็นสำคัญ

- ในระยะเวลา 2-3 ปีที่ผ่านมา ภาครัฐมีการจัดสรรงบประมาณในเชิงรุก แต่ควรบริหารงบประมาณในระดับหน่วยงานให้ดีขึ้น
- ต้องพิจารณาหาวิธีการดำเนินงานใหม่ๆ ให้แก่หน่วยงาน เพื่อให้เกิดการดำเนินงานอย่างมีประสิทธิภาพ
- การดำเนินงานที่มีมาตรฐานส่งผลให้ประหยัดค่าใช้จ่ายและสามารถจัดการโครงสร้างพื้นฐานได้ดีขึ้น นอกจากนี้ การดำเนินงานตามมาตรฐานยังสอดคล้องกับรูปแบบการดำเนินงานในอนาคตอีกด้วย

ทรัพยากรบุคคล

35% ของหน่วยงานระบุว่า ข้อจำกัดด้านศักยภาพบุคลากรและการฝึกอบรมเป็นอุปสรรคสำคัญ นอกจากนั้น แนวโน้มการเปลี่ยนงานที่สูงขึ้นของบุคลากรด้าน IT ที่ 12% นั้นเป็นอีกอุปสรรคที่สำคัญ เหตุผลอื่นที่สำคัญ ได้แก่ ค่าตอบแทนของภาครัฐไม่สามารถดึงดูดบุคลากรที่มีทักษะได้หากเทียบกับภาคเอกชน บุคลากรไม่เพียงพอต่อการดำเนินงานตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ รวมถึงศักยภาพและจำนวนบุคลากรไม่เพียงพอสำหรับการดูแลรักษา ฮาร์ดแวร์ ซอฟต์แวร์ และหน้าที่ IT อื่นๆ

ประเด็นสำคัญ

- ความท้าทายด้านทรัพยากรบุคคลเป็นเป็นอุปสรรคสำคัญต่อการปฏิบัติงานของหน่วยงานภาครัฐ โดยเฉพาะอย่างยิ่งบุคลากรด้าน IT ซึ่งมีความสำคัญในการขับเคลื่อนการดำเนินงานแต่มีจำนวนไม่เพียงพอ
- หน่วยงานต่างๆ จำเป็นต้องพิจารณาทางเลือกที่หลากหลายเพื่อรับมือกับการขาดบุคลากรที่มีทักษะเหมาะสม การได้รับค่าตอบแทนที่ต่ำ และการมีแนวโน้มการเปลี่ยนงานที่สูง นอกจากนี้ หน่วยงานจำเป็นต้องพิจารณาทางเลือกเพื่อสร้างความต่อเนื่องในการปฏิบัติงานและเพื่อรับมือกับงบประมาณที่ลดลง
- หน่วยงานต่างๆ อาจจำเป็นต้องพิจารณารูปแบบทางเลือกดังต่อไปนี้ 1) การใช้บริการจัดเก็บเครื่องแม่ข่ายไว้กับหน่วยงานภายนอก (Colocation) 2) การใช้บริการจัดเก็บข้อมูลไว้กับหน่วยงานภายนอก (3rd Party Services) และ 3) การใช้บริการโครงสร้างพื้นฐานของภาครัฐ (G-Services) ซึ่งเป็นรูปแบบการดำเนินงานในอนาคตเพื่อให้เกิดการปฏิบัติงานอย่างมีประสิทธิภาพ

การรักษาความปลอดภัยข้อมูล

หน่วยงานที่เข้าร่วมการประชุมระดมความคิดเห็นกลุ่มย่อยโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ระบุว่า การรักษาความปลอดภัยข้อมูลและการบริหารจัดการข้อมูลเป็นประเด็นสำคัญที่ต้องจัดการอย่างเหมาะสม เพื่อรักษาคุณภาพการให้บริการและประสิทธิภาพของโครงสร้างพื้นฐานภาครัฐ

ปัจจุบันภัยคุกคามและการโจมตีระบบคอมพิวเตอร์มีอยู่มากจากทั้งภายในและภายนอกประเทศซึ่งเป็นภัยคุกคามต่อศูนย์ข้อมูลภาครัฐ เนื่องจากระบบศูนย์ข้อมูลภาครัฐนั้นมีความสำคัญสูงสุดดังนั้นหน่วยงานภาครัฐจึงจำเป็นต้องใช้มาตรฐานการรักษาความปลอดภัยข้อมูลในระดับสูงสุด เพื่อป้องกันการโจมตีจากมัลแวร์และไวรัสที่สามารถรบกวนเครื่องแม่ข่ายและ

เครือข่าย ด้วยเหตุนี้ การรักษาความปลอดภัยจึงได้รับการจัดสรรงบประมาณให้เป็นจำนวนมากในหลายประเทศทั่วโลก นอกจากนั้น ประเด็นความท้าทายในการรักษาความปลอดภัยข้อมูลสามารถครอบคลุมถึงเครื่องคอมพิวเตอร์สำนักงาน ศูนย์ข้อมูลองค์กร และอุปกรณ์ไร้สายที่ใช้ปฏิบัติงาน เป็นต้น นอกจากนี้ ความท้าทายในการรักษาความปลอดภัยข้อมูลอาจรวมถึงความสามารถในการบูรณาการของข้อมูล ความมีประสิทธิภาพของระบบ ความสามารถในการเชื่อมโยงของระบบ และการรักษาความปลอดภัยใน Virtual Machine ทั้งนี้ การรักษาความปลอดภัยศูนย์ข้อมูลและระบบคลาวด์นั้น ต้องพิจารณาทั้งการรักษาความปลอดภัยในการรับและส่งข้อมูลระหว่างศูนย์ข้อมูล และการรับและส่งข้อมูลระหว่าง Virtual Machine อีกด้วย

จากผลการวิเคราะห์พบว่า 73% ของหน่วยงานมีความเห็นว่าในปัจจุบันหน่วยงานของตนมีปัญหาด้านความปลอดภัยในบางประการหรือเล็กน้อย ในขณะที่อีก 15% เชื่อว่าหน่วยงานของตนไม่ได้จัดการข้อมูลที่ต้องการความปลอดภัยสูงได้อย่างมีประสิทธิภาพเพียงพอ การรักษาความปลอดภัยข้อมูลนั้นถือเป็นหนึ่งในเรื่องที่สำคัญที่สุด ซึ่งหน่วยงานภาครัฐในหลายประเทศกำลังเผชิญกับปัญหานี้ ส่วนในประเทศไทยนั้น หน่วยงานภาครัฐมีความใส่ใจด้านการรักษาความปลอดภัยข้อมูลที่สูงขึ้นแต่ยังกังวลต่อการรักษาความปลอดภัยข้อมูลของระบบคลาวด์อยู่

15% *ของผู้ตอบแบบสอบถามระบุว่าหน่วยงานของตนไม่จัดการแอปพลิเคชันที่ต้องการความปลอดภัยสูงได้อย่างเหมาะสม*

ประเด็นสำคัญ

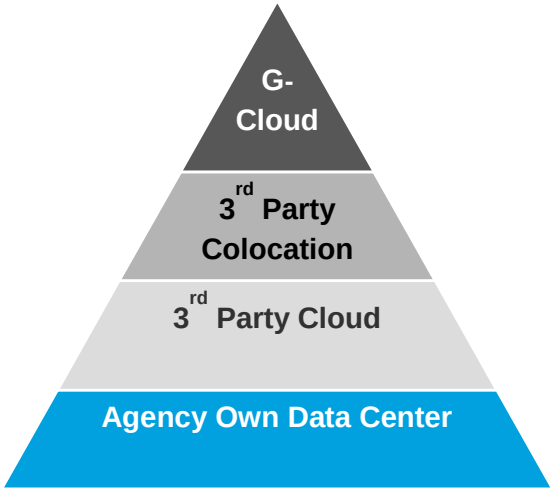
- การรักษาความปลอดภัยคือความท้าทายสำคัญสำหรับหน่วยงานภาครัฐทั่วโลกรวมทั้งประเทศไทย
- การขาดการรักษาความปลอดภัยที่มีประสิทธิภาพก่อให้เกิดความเสี่ยงต่อความปลอดภัยของโครงสร้างพื้นฐานและข้อมูลที่เป็นความลับของประเทศ
- โครงการการพัฒนาศูนย์ข้อมูลภาครัฐนี้ควรเป็นส่วนช่วยให้เกิดโครงสร้างพื้นฐานที่มีการรักษาความปลอดภัยและปฏิบัติงานในสภาพแวดล้อมที่มีความปลอดภัย
- โครงสร้างพื้นฐานทางกายภาพต้องได้รับการรักษาความปลอดภัยที่ดีขึ้น มีความสอดคล้องกับกฎระเบียบ และมีกระบวนการที่ทำให้เป็นมาตรฐานสำหรับอนาคต
- ข้อมูลต้องถูกเก็บรักษาจากทางเลือกที่หลากหลายและตรงต่อความต้องการทางด้านการรักษาความปลอดภัยที่เหมาะสมสำหรับหน่วยงาน

โครงสร้างพื้นฐานและการจัดการข้อมูลของหน่วยงาน

หน่วยงานภาครัฐต่างเล็งเห็นถึงความสำคัญและความจำเป็นที่ต้องเปลี่ยนแปลงไปใช้โครงสร้างพื้นฐานที่มีประสิทธิภาพสูงขึ้น โดยโครงสร้างพื้นฐานในปัจจุบันของหน่วยงานมีดังนี้ 1) ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) 2) การใช้บริการคลาวด์ภาครัฐ (G-Cloud) 3) การใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) และ 4) การใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) จาก 42 หน่วยงานทั้งหมดที่ตอบแบบสำรวจในการประชุมระดมความคิดเห็นกลุ่มย่อยโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) นั้น 90% ของหน่วยงานระบุว่าหน่วยงานของตนใช้ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) ในการจัดเก็บและประมวลผลข้อมูล ขณะที่อีก 20% ระบุว่าหน่วยงานของตนใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) และบริการคลาวด์ภาครัฐ G-Cloud โดยที่มีเพียง 7% ของหน่วยงานที่ระบุว่าใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud)

โครงสร้างพื้นฐานของหน่วยงานเป็นองค์ประกอบสำคัญที่ส่งผลให้ภาครัฐปฏิบัติงานได้อย่างมีประสิทธิภาพ ซึ่งโครงสร้างพื้นฐานนั้นครอบคลุมศูนย์ข้อมูล เครื่องแม่ข่าย เครือข่ายสื่อสารข้อมูล (Data Communication) ระบบ Virtual Private Network (VPN) และเครือข่ายบริการโทรคมนาคมอื่นๆ

ปัจจุบันหน่วยงานภาครัฐของไทยบริหารจัดการข้อมูลโดยอาศัยโครงสร้างพื้นฐานด้านข้อมูลใน 4 รูปแบบต่อไปนี้



- 4 รูปแบบนี้รองรับศูนย์ข้อมูลและโครงสร้างพื้นฐานด้านข้อมูลของประเทศไทยในปัจจุบัน
- Agency Own Data Center เป็นโครงสร้างพื้นฐานที่ใช้งานอย่างแพร่หลายที่สุด โดยข้อมูลถูกจัดเก็บภายในหน่วยงานเอง และหน่วยงานบริหารการรักษาความปลอดภัยเอง
- 3rd Party Cloud เป็นอีกหนึ่งโครงสร้างพื้นฐานที่สำคัญ โดยมีแอปพลิเคชันจำนวน 64 แอปพลิเคชันที่ถูกจัดเก็บบนระบบคลาวด์ของหน่วยงานภายนอก (ข้อมูลสถานะปี ค.ศ. 2014)
- 3rd Party Colocation ถือเป็นอีกทางเลือกที่สำคัญโดยหน่วยงานจัดจ้างหน่วยงานภายนอกเพื่อดูแลรักษาและจัดการความปลอดภัย โดยมีเครื่องแม่ข่ายมากกว่า 300 เครื่องที่ใช้บริการเช่าพื้นที่วาง
- G-Cloud ให้บริการแก่แอปพลิเคชันถึง 109 แอปพลิเคชัน (ข้อมูลสถานะปี ค.ศ. 2014)

ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center)

โครงสร้างพื้นฐานของหน่วยงานภาครัฐในปัจจุบันนั้นนิยมใช้ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) จากการวิเคราะห์ข้อมูลที่ได้รับจากหน่วยงานต่างๆ ประมาณ 92% ของหน่วยงานมีการปฏิบัติงานโดยมีศูนย์ข้อมูลของตนเอง หลายหน่วยงานมีความเห็นว่าการมีศูนย์ข้อมูลประจำหน่วยงานนั้นทำให้หน่วยงานมีความสามารถในการรองรับการดำเนินงานที่เพิ่มขึ้นและสามารถรักษาความปลอดภัยไปพร้อมกันได้ หน่วยงานที่จัดการข้อมูลทางการเงินหรือข้อมูลที่เป็นความลับมักนิยมใช้ศูนย์ข้อมูลประจำหน่วยงาน นอกจากนี้ หน่วยงานต่างๆ ที่มีศูนย์ข้อมูลเป็นของตนเอง ยังไม่เห็นถึงความไม่จำเป็นในการใช้บริการศูนย์ข้อมูลของหน่วยงานอื่นเพื่อเก็บข้อมูล และแอปพลิเคชันบางชนิดไม่สามารถจัดเก็บบนระบบคลาวด์ภาครัฐ G-Cloud ได้อีกด้วย

ประเด็นสำคัญ

- แม้ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) ถือเป็นโครงสร้างพื้นฐานที่นิยมที่สุดของหน่วยงาน แต่หน่วยงานต้องคำนึงถึงทางเลือกอื่นๆ ในการจัดเก็บข้อมูลด้วย เช่น G-Services เป็นต้น
- ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) เพิ่มความสะดวกในการจัดการความปลอดภัยของหน่วยงานเอง แต่ศูนย์ข้อมูลแบบดังกล่าวก่อให้เกิดปัญหาด้านงบประมาณ การบำรุงรักษา การหยุดชะงักของการให้บริการ ความพร้อมใช้งาน และประสิทธิภาพของการให้บริการ
- ในการปฏิบัติตามมาตรฐาน ศูนย์ข้อมูลจำเป็นต้องบริหารค่าใช้จ่ายอย่างมีประสิทธิภาพเพื่อความคุ้มค่าในการลงทุน
- ศูนย์ข้อมูล เครื่องแม่ข่าย และโครงสร้างพื้นฐานที่ล้าสมัยอาจมีความเสี่ยงด้านความปลอดภัย และอาจไม่คุ้มค่าเนื่องจากมีค่าบำรุงรักษาที่สูง
- การลงทุนเพื่อปรับปรุงศูนย์ข้อมูลจะก่อให้เกิดค่าใช้จ่าย CAPEX ที่สูง
- กล่าวโดยสรุป ทิศทางในอนาคตเกี่ยวกับโครงสร้างพื้นฐานของหน่วยงานควรคำนึงถึงมิติต่างๆ โดยเฉพาะอย่างยิ่งความเสี่ยงที่อาจเกิดขึ้น เช่น ข้อมูลสูญหายหรือรั่วไหล เป็นต้น

การใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud)

โครงสร้างพื้นฐานของหน่วยงานภาครัฐในปัจจุบันมีการใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) ที่ให้บริการโดยบริษัทเอกชนหลายแห่งในประเทศไทยเพื่อรองรับแอปพลิเคชันของหน่วยงาน

ประเด็นสำคัญ

- ควรมุ่งเน้นการใช้ทรัพยากรให้เกิดประโยชน์สูงสุด เช่น การให้บริการที่มีคุณค่าแก่ผู้ใช้บริการ
- หน่วยงานต่างๆ ควรใช้ระบบที่มีความยืดหยุ่น ที่มีความสามารถรองรับข้อมูลและผู้ใช้งานเพิ่มขึ้น มีการรักษาความปลอดภัยในระดับสูง
- การให้บริการคลาวด์โดยหน่วยงานภายนอกอาจไม่น่าเชื่อถือด้านการจัดการความปลอดภัย แต่ในทางกลับกัน การให้บริการดังกล่าวได้รับความเชื่อมั่นว่ามีพัฒนาการในการบริการ ทั้งในเรื่องเทคโนโลยี และการรักษาความความปลอดภัยที่ดีขึ้นอย่างต่อเนื่อง
- ข้อดีของการทำ Virtualization คือ ความยืดหยุ่นในการเพิ่มทรัพยากรและขยายบริการ การประหยัดพลังงาน และค่าใช้จ่าย ซึ่งล้วนเป็นประโยชน์จากการนำระบบคลาวด์มาใช้
- การให้บริการคลาวด์โดยหน่วยงานภายนอกนั้นช่วยให้หน่วยงานสามารถลดความยุ่งยากต่างๆ ได้ เช่น การกู้คืนภัยพิบัติ การอัพเดต การจัดซื้อซอฟต์แวร์ ความสามารถในการขยายการให้บริการ ค่าใช้จ่ายในการลงทุน การควบคุมเอกสาร และการจัดการความปลอดภัย เป็นต้น
- ถึงแม้ความปลอดภัยของการบริการคลาวด์อาจเป็นอุปสรรคต่อการจัดเก็บข้อมูลสำคัญและข้อมูลด้านความมั่นคงของประเทศ แต่ข้อมูลทั่วไปสามารถใช้วิธีการจัดเก็บแบบดังกล่าวได้ ระบบคลาวด์สามารถจัดการข้อมูลด้วยค่าใช้จ่ายที่ต่ำกว่า มีความพร้อมใช้งาน และมีเสถียรภาพสูง
- ข้อดีของการให้บริการคลาวด์โดยหน่วยงานภายนอกคือ การลดภาระทรัพยากรบุคคลและการดำเนินงานรายวัน ซึ่งเป็นปัญหาสำคัญของหน่วยงานภาครัฐไทยในปัจจุบัน

การใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation)

หน่วยงานไทยมีการใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) โดยที่เครื่องแม่ข่ายจำนวน 324 เครื่องของภาครัฐ (ข้อมูลสถานะปี ค.ศ. 2014) ถูกจัดเก็บไว้กับหน่วยงานภายนอก การใช้บริการวางเครื่องแม่ข่ายถือเป็นแนวทางขั้นพื้นฐานที่สำคัญสำหรับหน่วยงานต่างๆ ในประเทศไทย หลายหน่วยงานมีความประสงค์ที่จะใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอกอย่างชัดเจนเพราะความสะดวกในหลายด้าน เช่น การรักษาความปลอดภัยที่สูงกว่า การลดข้อจำกัดในการจัดการ และทรัพยากรบุคคล เป็นต้น

ประเด็นสำคัญ

- 3rd Party Colocation เป็นทางเลือกในการจัดเก็บข้อมูลที่เหมาะสมสำหรับหลายหน่วยงาน
- หน่วยงานควรพิจารณาเลือกแอปพลิเคชัน เครื่องแม่ข่าย และประเภทข้อมูลที่มีความเหมาะสมในการจัดเก็บไว้กับผู้ให้บริการ 3rd Party Colocation
- หน่วยงานจำเป็นที่ต้องเข้าใจในข้อตกลงระดับการให้บริการ (SLA) ที่ผู้ให้บริการ 3rd Party Colocation ใช้ปฏิบัติงานอย่างถ่องแท้
- 3rd Party Colocation อาจไม่ได้รับความเชื่อมั่นจากผู้ใช้บริการในเรื่องการจัดการความปลอดภัยข้อมูล แต่พบว่ามีปัญหาน้อยกว่าที่หน่วยงานได้รับจากบริการ 3rd Party Cloud
- บริการ Colocation เป็นตัวเลือกที่เหมาะสมสำหรับหน่วยงานที่มีห้องเครื่องแม่ข่ายขนาดเล็กหรือมีโครงสร้างพื้นฐานที่เล็กกว่าหน่วยงานอื่น แต่มีความต้องการที่จะเพิ่มโครงสร้างพื้นฐานอย่างเร่งด่วนหรือจำเป็นต้องปรับปรุงโครงสร้างพื้นฐานเพื่อรองรับข้อมูลหรือแอปพลิเคชันที่ต้องการความปลอดภัยหรือมีความสำคัญต่อพันธกิจสูงขึ้น

การใช้บริการคลาวด์ภาครัฐ (G-Cloud)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) เป็นผู้ให้บริการคลาวด์ภาครัฐ (G-Cloud) ซึ่งเป็นโครงสร้างพื้นฐานด้าน IT ที่สามารถใช้งานจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ใช้บริการคลาวด์ภาครัฐ (G-Cloud) จะได้รับระดับการรักษาความปลอดภัยที่สูงกว่า แต่มีค่าใช้จ่ายด้านบุคลากรต่ำกว่า

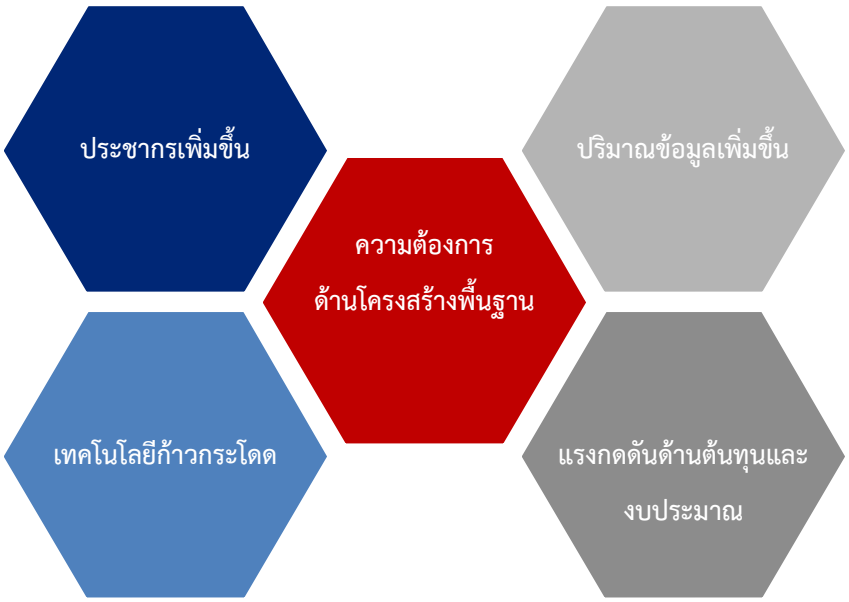
ประเด็นสำคัญ

- G-Cloud ถือเป็นโครงสร้างพื้นฐานสำคัญที่หน่วยงานต่างๆ กำลังพิจารณาย้ายแอปพลิเคชันไปใช้งานมากขึ้นเรื่อยๆ
- ความปลอดภัยของข้อมูล ความเสถียร และความพร้อมใช้งาน เป็นประเด็นสำคัญที่ G-Cloud จำเป็นต้องพัฒนาอย่างต่อเนื่อง
- G-Cloud จะเป็นโครงสร้างพื้นฐานที่มีบทบาทสำคัญในอนาคตเนื่องจากเป็นทางเลือกที่เหมาะสมสำหรับการลดค่าใช้จ่ายในการบำรุงรักษา การจัดซื้ออุปกรณ์ อีกทั้งหน่วยงานสามารถใช้บริการได้อย่างมีประสิทธิภาพ
- G-Cloud ควรคำนึงถึงการจำแนกประเภทและการบูรณาการข้อมูล
- G-Cloud ควรให้บริการตามมาตรฐานในการจัดเก็บข้อมูลทั่วไป และสามารถยกระดับมาตรฐานการจัดการข้อมูลให้สูงขึ้นในระยะยาวได้
- G-Cloud ควรรักษามาตรฐานในระยะยาว ความพร้อมใช้งานตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ มีระบบช่วยเหลือผู้ใช้งาน และคุณลักษณะทั้งหมดที่ 3rd Party Cloud ให้บริการ โดยมีระดับการจัดการความปลอดภัยสูงที่ขึ้นและค่าใช้จ่ายที่ต่ำลง

9. โครงสร้างพื้นฐานด้านข้อมูลของประเทศไทยในอนาคต

ปัจจุบันประเทศไทยอยู่ระหว่างการยกระดับทางเศรษฐกิจ รัฐบาลขับเคลื่อนการพัฒนาประเทศในทุกภาคส่วนซึ่งเป็นตัวชี้วัดสำคัญที่แสดงถึงความมุ่งมั่นเพื่อให้บรรลุเป้าหมาย ความสามารถในการแข่งขันของประเทศไทยในเวทีโลกนั้นมีอันดับสูงขึ้นซึ่งนับเป็นสัญญาณที่ดีที่สะท้อนถึงความสำเร็จของประเทศในด้านเศรษฐกิจระดับนานาชาติที่เชื่อมโยงกับเศรษฐกิจภายในประเทศ ปี ค.ศ. 2016 (IMD World Competitiveness Ranking 2016) เศรษฐกิจของประเทศไทยอยู่ในอันดับที่ 28 จากทั้งหมด 61 ประเทศที่คะแนนรวม 74.681 ซึ่งขึ้นจากอันดับที่ 30 ในปี ค.ศ. 2015 ที่คะแนนรวม 69.786 นอกจากนั้น ในปี ค.ศ. 2015 ประเทศไทยนับเป็นประเทศสมาชิกอาเซียนเพียงประเทศเดียวที่มีอันดับสูงขึ้นกว่าปีที่ผ่านมา ที่สำคัญที่สุด ประเทศไทยอยู่ระหว่างการเร่งดำเนินโครงการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี สาธารณสุข และสิ่งแวดล้อมที่มุ่งเน้นนวัตกรรมและอุตสาหกรรมประหยัดพลังงาน (Green Industry) นอกจากนั้น ประเทศไทยเป็นสมาชิกกลุ่มเศรษฐกิจภูมิภาคเอเชียตะวันออกเฉียงใต้ (Southeast Asia) และเอเชียตะวันออก (East Asia) มาเป็นเวลานานซึ่งเป็นศูนย์กลางการวิจัยและเป็นส่วนผลักดันการเติบโตทางเศรษฐกิจของโลก โดย International Monetary Fund (IMF) คาดการณ์ว่าอัตราการเติบโตทางเศรษฐกิจของประเทศไทยในปีนี้ (ค.ศ. 2017) นั้นจะอยู่ที่ 3.3%

ด้วยเศรษฐกิจที่เคลื่อนไหวอยู่ตลอดเวลาและการมุ่งเน้นนโยบายเศรษฐกิจดิจิทัล (Digital Economy) ของภาครัฐนั้นจะผลักดันให้โครงสร้างพื้นฐานของหน่วยงานภาครัฐในประเทศก้าวสู่การพัฒนาที่ดีขึ้น



ดังเช่นในประเทศอื่นๆ การเพิ่มของจำนวนประชากรมักส่งผลให้ความต้องการบริการโครงสร้างพื้นฐานดิจิทัล การใช้ Data Analytics และความคาดหวังต่อภาครัฐนั้นเพิ่มขึ้น ซึ่งปัจจัยที่กล่าวมานี้จะส่งผลให้เกิดความต้องการโครงสร้างพื้นฐานศูนย์ข้อมูลขนาดใหญ่ ดังนั้น ภาครัฐจึงจำเป็นต้องพิจารณาปัจจัยดังกล่าวเพื่อรองรับการเติบโตของประเทศไทย

เทคโนโลยีก้าวหน้าอย่างรวดเร็วกว่าที่ผ่านมาซึ่งสามารถกำหนดความต้องการโครงสร้างพื้นฐาน นอกจากนี้ ความก้าวหน้าทางเทคโนโลยีแห่งอนาคตจะช่วยให้ประเทศใช้ประโยชน์จากข้อมูลและโครงสร้างพื้นฐานที่มีอยู่ได้อย่างมีประสิทธิภาพมากขึ้น เช่น จาก Smart Devices, Internet of Things, Sensors และ Smart Meters เป็นต้น นอกจากนี้ ความก้าวหน้าทางเทคโนโลยีแห่งอนาคตยังช่วยให้ประเทศสามารถเลือกใช้โครงสร้างพื้นฐานที่ดีกว่าเดิมอีกด้วย

เนื่องด้วยต้นทุนการบริการสูงขึ้น การบริการด้านโครงสร้างพื้นฐานจึงมีราคาสูงขึ้นตามตัว นอกจากนี้ ต้นทุนการบริการที่สูงขึ้นนั้นเกิดขึ้นกับทุกประเทศทั่วโลก ซึ่งหน่วยงานภาครัฐไม่สามารถหลีกเลี่ยงปัญหาดังกล่าวได้หากต้นทุน หรือการอนุมัติงบประมาณ และการรัดเข็มขัดยังเป็นปัญหาหรือยังไม่ได้รับการแก้ไข

ปริมาณข้อมูลนั้นเพิ่มขึ้นหลายเท่าตัวในทุกๆ ปี ซึ่งปรากฏการณ์นี้ไม่เพียงเป็นผลจากจำนวนประชากรที่เพิ่มสูงขึ้น แต่เป็นผลจากประสิทธิภาพที่สูงขึ้นของโครงสร้างพื้นฐานดิจิทัล อุปกรณ์เชื่อมต่ออินเทอร์เน็ต แอปพลิเคชัน และการบริการออนไลน์ เป็นต้น นอกจากนี้ การทำธุรกรรมทางการเงิน การบริการแลกเปลี่ยนข้อมูล การวิเคราะห์ข้อมูล และความต้องการบริการที่เพิ่มขึ้นล้วนผลักดันให้ปริมาณข้อมูลขยายตัวอย่างมหาศาล หากโครงสร้างพื้นฐานที่รองรับข้อมูลเหล่านี้ยังคงรูปแบบการดำเนินการแบบเดิม การปฏิบัติงานภาครัฐในอนาคตจะขาดประสิทธิภาพทั้งการดำเนินงานและต้นทุน

คุณสมบัติของโครงสร้างพื้นฐานในอนาคต (Maturity Parameters of Future Infrastructure)

ทิศทางอนาคตของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทยมีนิยามว่า โครงสร้างพื้นฐานที่ทำขึ้นใหม่จากการพัฒนาองค์ประกอบต่างๆ เช่น วิสัยทัศน์และเป้าหมายของภาครัฐ ยุทธศาสตร์โครงสร้างพื้นฐานด้านข้อมูล โครงสร้างพื้นฐานปัจจุบัน ความคาดหวังและความต้องการของประชาชนและหน่วยงานภาครัฐ ความเสี่ยงและความท้าทายที่ภาครัฐเผชิญในปัจจุบันและในอนาคต

ทิศทางอนาคตของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐถูกดำเนินงานภายใต้โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) นั้นประกอบด้วย 5 คุณลักษณะที่โดดเด่นและมีความแตกต่างจากโครงสร้างพื้นฐานเดิม ซึ่งจะเป็นรากฐานสำคัญสำหรับยุทธศาสตร์ในอนาคต

การจัดการความปลอดภัยอย่างมีประสิทธิภาพ (Security Handling)

การจัดการความปลอดภัยอย่างมีประสิทธิภาพเป็นคุณลักษณะสำคัญที่สุดประการหนึ่งและเป็นข้อกำหนดสำหรับรูปแบบการดำเนินงานในอนาคตที่มีความสำคัญต่อทิศทางอนาคตของโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทย

การจัดการความปลอดภัยอย่างมีประสิทธิภาพ ได้แก่ การรักษาความปลอดภัยและการป้องกันการนำข้อมูลด้านความมั่นคงไปใช้ การใช้เทคโนโลยีการเข้ารหัส (Encryption) การใช้เทคโนโลยีรักษาความปลอดภัยในการรับส่งข้อมูล การรักษาความปลอดภัยข้อมูลสำคัญต่อพันธกิจ (Mission Critical Data) และการจัดการข้อมูลทั่วไปอย่างมีประสิทธิภาพ

คุณลักษณะสำคัญสำหรับทิศทางอนาคต

โครงสร้างพื้นฐานในอนาคตควรปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่ระบุไว้ในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards) โดยครอบคลุมความปลอดภัยของข้อมูล ความปลอดภัยสารสนเทศ และความปลอดภัยทางกายภาพ

โครงสร้างพื้นฐานในอนาคตแต่ละด้านควรถูกบริหารจัดการตามความสามารถและศักยภาพในการจัดการความปลอดภัย

หน่วยงานภาครัฐจำเป็นต้องจำแนกประเภทและกำกับดูแลข้อมูลอย่างเหมาะสม เพื่อการตัดสินใจทิศทางการดำเนินงานในอนาคต

การดำเนินงานในอนาคตสามารถใช้โครงสร้างพื้นฐานได้อย่างเต็มที่ หากโครงสร้างพื้นฐานนั้นมีความทันสมัย มีการจัดการข้อมูลอย่างปลอดภัย และมีการปฏิบัติงานภายใต้ความเสี่ยงที่น้อยลง

ความสามารถในการรองรับการขยายตัวของบริการ (Scalability)

ข้อมูลที่มีปริมาณเพิ่มมากขึ้นจากหลายช่องทาง โครงสร้างพื้นฐานด้านข้อมูลต้องตระหนักถึงความสำคัญของความสามารถในการรองรับการขยายตัวของบริการสำหรับข้อมูลเหล่านั้น โดยในระยะเวลา 2-3 ปีที่ผ่านมา การพัฒนาแอปพลิเคชันมีการขยายตัวเกือบเท่ากับการลงทุนด้านโครงสร้างพื้นฐานและการจัดตั้งศูนย์ข้อมูล ในปัจจุบันศูนย์ข้อมูลมีอัตราการใช้งานพื้นที่และอัตราการการใช้ประโยชน์ในระดับที่ต่ำ นอกจากนี้ปัจจัยสำคัญที่ทำให้ศูนย์ข้อมูลสามารถรองรับปริมาณข้อมูลที่มากขึ้นอย่างทันท่วงทีคือความสามารถในการรองรับการขยายตัวของบริการ (Scalability) นั่นเอง

ความสามารถในการรองรับการขยายตัวของบริการ (Scalability) คือ หน่วยงานภาครัฐมีทางเลือกหลากหลายในการจัดเก็บแอปพลิเคชันตามขนาดพื้นที่จัดเก็บที่เปลี่ยนแปลงไปและตรงกับความต้องการ นอกจากนี้ความสามารถในการรองรับการขยายตัวของบริการทำให้เกิดเสถียรภาพในการให้บริการ กรณีที่แอปพลิเคชันซับซ้อนมากขึ้น ชนิดของข้อมูลหลากหลายมากขึ้น และความต้องการพื้นที่จัดเก็บข้อมูลรวมถึงความสามารถในการประมวลผลที่สูงขึ้น นอกจากนี้ โครงสร้างพื้นฐานที่มีความสามารถในการรองรับการขยายตัวของบริการนั้นสามารถรองรับความต้องการได้อย่างสะดวกรวดเร็ว (Plug-and-Play) และค่าบริการเหมาะสมตามการใช้งานจริง (Pay-as-You-Go)

คุณลักษณะสำคัญสำหรับทิศทางอนาคต

โครงสร้างพื้นฐานในอนาคตควรมีทางเลือกในการรองรับการขยายตัวของบริการ (Scalability) ตามความต้องการ

โครงสร้างพื้นฐานในอนาคตแต่ละด้านจะบริหารจัดการตามความสามารถในการรองรับการขยายตัวของบริการเพื่อให้หน่วยงานภาครัฐสามารถตัดสินใจอย่างถูกต้อง

ความสามารถในการรองรับการขยายตัวของบริการส่งผลให้อัตราการใช้ประโยชน์โครงสร้างพื้นฐานด้านข้อมูลและอัตราการใช้ประโยชน์จาก CAPEX/OPEX ของภาครัฐในอนาคตนั้นสูงขึ้น นอกจากนี้ หน่วยงานที่ต้องการรองรับการขยายตัวของบริการนั้นควรใช้ระบบที่มีความสามารถดังกล่าวแทนการลงทุน CAPEX เนื่องจากมีการเสื่อมราคา

ต้องมีการทำความสะอาดและจำแนกประเภทข้อมูล (Data Cleasing and Classification) เพื่อใช้งานพื้นที่จัดเก็บให้มีประสิทธิภาพสูงสุด

การออกแบบเพื่อรองรับอนาคต (Designed For Future)

ทิศทางในอนาคตสำหรับโครงสร้างพื้นฐานด้านข้อมูลของภาครัฐไทยควรมีความยั่งยืน มีการส่งเสริมการนำเทคโนโลยีใหม่มาใช้ ก่อให้เกิดนวัตกรรมเปิด (Open Innovation) และมีมาตรฐาน นอกจากนี้ หากพิจารณาจากมุมมองด้านสถาปัตยกรรมองค์กร (Enterprise Architecture) วิธีการรับส่งข้อมูลระหว่างกระบวนการนั้นมีความสำคัญเป็นอย่างยิ่ง โดยเฉพาะการเตรียมการเพื่อการแลกเปลี่ยนหรือใช้ข้อมูลร่วมกันในอนาคต

ในปัจจุบันนั้น แอปพลิเคชันมีการส่งข้อมูลระหว่างกันซึ่งการเชื่อมต่อแอปพลิเคชันต้องได้รับการออกแบบที่ดี นอกจากนี้ การทำ Virtualization เป็นที่นิยมมากขึ้น ซึ่งทั้งหมดที่กล่าวมาล้วนเป็นการทำให้ระบบเครือข่ายถูกใช้งานอย่างเต็มประสิทธิภาพและก่อให้เกิดการรับส่งข้อมูลระหว่างศูนย์ข้อมูลและ Virtual Machine เพิ่มมากขึ้น

ในอดีต เวลาที่ยอมรับได้เพื่อให้แอปพลิเคชันทำงานนั้นใช้เป็นหน่วยวินาที แต่เวลาสำหรับแอปพลิเคชันสมัยใหม่นั้นจำเป็นต้องทำงานในเวลาเป็นหน่วยมิลลิวินาที (Millisecond) และอาจยิ่งเร็วกว่านี้ในอนาคตอันใกล้ ประเด็นของเวลานั้นมีความสำคัญมากขึ้นสำหรับแอปพลิเคชันที่เน้นการให้บริการแก่ประชาชนและการให้บริการธุรกรรมทางการเงิน นอกจากนี้ ปริมาณการรับส่งข้อมูลจะเพิ่มขึ้นจากการผสมผสานการใช้งาน Data Analytics, Big Data, และ Internet of Things (IoT) เข้าด้วยกัน

การออกแบบเพื่อรองรับอนาคตคือ ความสามารถที่ทำให้โครงสร้างพื้นฐานด้านข้อมูลสามารถรองรับการบริการแก่ประชาชนได้อย่างรวดเร็วและทันต่อความต้องการในอนาคต ซึ่งความสามารถหลักได้แก่ ความสามารถในการใช้เทคโนโลยีคลาวด์มากขึ้นและความสามารถในการอัพเกรดแอปพลิเคชันได้ดีขึ้น นอกจากนี้แอปพลิเคชันแบบใหม่นั้นมักถูกพัฒนาขึ้นโดยการใช้เทคโนโลยี Virtualization, Container และ Micro-Services โดยสามารถเชื่อมต่อกับระบบภายนอกได้ง่ายขึ้นซึ่งต่างจากแอปพลิเคชันที่มีอยู่เดิมโดยสิ้นเชิง

คุณลักษณะสำคัญสำหรับทิศทางอนาคต

โครงสร้างพื้นฐานในอนาคตควรดำเนินงานตามมาตรฐานที่กำหนดในด้านพลังงานไฟฟ้า สถานที่ตั้ง การออกแบบ และการเพิ่มประสิทธิภาพ ซึ่งมาตรฐานเหล่านี้ได้รับการพัฒนาขึ้นอย่างรอบคอบโดยพิจารณาจากสถานะปัจจุบัน ผลตอบแทนการลงทุน ต้นทุน และการวางแผนระยะยาว

โครงสร้างพื้นฐานที่รองรับความต้องการในอนาคตควรสนับสนุนนวัตกรรม เทคโนโลยี และแอปพลิเคชันใหม่ๆ

โครงสร้างพื้นฐานควรถูกพัฒนาขึ้นโดยพิจารณาถึงความซับซ้อนของข้อมูลที่เกิดจาก Data Analytics ข้อมูลที่ได้รับจากอุปกรณ์ IoT และข้อมูลจากแหล่งอื่นๆ

โครงสร้างพื้นฐานสำหรับอนาคตต้องมีบุคลากรที่เข้าใจระบบเหล่านี้และเข้าใจถึงการเปลี่ยนแปลงต่างๆ ได้อย่างรวดเร็ว หน่วยงานควรมีความสามารถปรับเปลี่ยนตัวเลือกต่างๆ ในด้านโครงสร้างทั้งเชิงบริหาร ระบบ และกายภาพ เพื่อรองรับความต้องการในอนาคตได้อย่างมีประสิทธิภาพ

ควรพิจารณาด้านสถานที่ตั้งศูนย์ข้อมูล (สำหรับกรณีที่สร้างใหม่) นอกจากนี้ สถานที่ตั้งของศูนย์ข้อมูลที่ให้บริการระหว่าง

หน่วยงานนั้นควรมีการศึกษาและวิเคราะห์ความเป็นไปได้ก่อนดำเนินการออกแบบ

การเพิ่มประสิทธิภาพด้านต้นทุน (Cost Optimization)

หน่วยงานต้องพิจารณาลดค่าใช้จ่ายหรือใช้งบประมาณอย่างคุ้มค่าที่สุดเนื่องจากต้นทุนการให้บริการนั้นสูงขึ้น เป็นผลมาจากปริมาณข้อมูลที่เพิ่มขึ้นและเทคโนโลยีที่มีราคาสูงขึ้น นอกจากนี้ต้นทุนที่สูงขึ้นของพื้นที่ศูนย์ข้อมูล พลังงาน ทรัพยากรบุคคล ความซ้ำซ้อนของโครงสร้างพื้นฐาน การใช้งานไม่เต็มประสิทธิภาพ และแผนพัฒนาเศรษฐกิจดิจิทัล (Digital Economy) ล้วนกระตุ้นการเพิ่มประสิทธิภาพด้านต้นทุน (Cost Optimization) อย่างไรก็ดี การเพิ่มประสิทธิภาพด้านต้นทุนนั้นมิใช่แค่การจำกัดงบประมาณด้านโครงสร้างพื้นฐานอย่างที่ปฏิบัติกันในหลายๆ ประเทศเท่านั้น

การเพิ่มประสิทธิภาพด้านต้นทุน (Cost Optimization) คือ การใช้ทรัพยากรภาครัฐอย่างมีประสิทธิภาพจากงบประมาณที่เหมาะสม การบำรุงรักษาโครงสร้างพื้นฐานให้ได้มากที่สุด การใช้ประโยชน์จากทางเลือกต่างๆ เพื่อประหยัดค่าใช้จ่าย การพึ่งพาเทคโนโลยีที่มี CAPEX ต่ำเพื่อหลีกเลี่ยงความเสื่อมราคา และการวางแผนการบริหารจัดการข้อมูลในระยะยาวที่ดี

การเพิ่มประสิทธิภาพด้านต้นทุนคือ การหาทางเลือกต่างๆ เพื่อใช้โครงสร้างพื้นฐานร่วมกัน การใช้บริการพื้นที่วางเครื่องแม่ข่าย (Colocation) และการทำ Virtualization เพื่อลดค่าใช้จ่ายและยกระดับคุณภาพการให้บริการ ดังนั้นการจัดจ้างหน่วยงานภายนอกเพื่อให้บริการ (Outsource) และการเลือกใช้ระบบคลาวด์นั้นจึงเป็นทางเลือกที่เหมาะสมสำหรับการดำเนินงานโดยไม่ส่งผลกระทบต่อคุณภาพและเป้าหมายของการบริการ

คุณลักษณะสำคัญสำหรับทิศทางอนาคต

โครงสร้างพื้นฐานในอนาคตควรมีการวางแผนเพื่อให้เกิดการลงทุนอย่างมีประสิทธิภาพโดยลด CAPEX ที่ต้องใช้ในฮาร์ดแวร์และซอฟต์แวร์

ประสิทธิภาพด้านต้นทุนของแอปพลิเคชันและข้อมูลควรจะมีความสมดุลกันกับแพลตฟอร์มและเทคโนโลยีที่เลือกใช้

แนวทางด้านความปลอดภัยจะต้องมีการปฏิบัติตามเพื่อให้หน่วยงานสามารถเลือกใช้ระบบรักษาความปลอดภัยที่เหมาะสมกับประเภทของข้อมูลและงบประมาณ

ค่าใช้จ่าย OPEX ควรต้องลดลงในการให้บริการบางชนิดของหน่วยงาน นอกจากนี้ อัตราการใช้งานโครงสร้างพื้นฐานจะเพิ่มขึ้นหากหน่วยงานใช้งานโครงสร้างพื้นฐานร่วมกัน

การดำเนินงานอย่างมีประสิทธิภาพ (Operational Efficiency)

การใช้ประโยชน์ศูนย์ข้อมูลอย่างมีประสิทธิภาพนั้นเป็นเรื่องสำคัญในการจัดการโครงสร้างพื้นฐานภาครัฐ การเพิ่มประสิทธิภาพการใช้พลังงานไฟฟ้าของศูนย์ข้อมูลเป็นเรื่องสำคัญ แต่หน่วยงานภาครัฐส่วนใหญ่ยังเผชิญปัญหาเนื่องจากค่าไฟฟ้าที่เพิ่มขึ้น นอกจากนี้ศูนย์ข้อมูลที่สร้างขึ้นก่อนมีการนำเทคโนโลยี Virtualization มาใช้ อาจมีพื้นที่เกินความต้องการในปัจจุบัน ดังนั้น จึงถือเป็นโอกาสที่หน่วยงานจะลดพื้นที่ อุปกรณ์ และพลังงานที่ใช้ในศูนย์ข้อมูลนั้น ที่สำคัญ หากบุคลากรมีประสิทธิภาพมากขึ้น ศูนย์ข้อมูลสามารถรองรับการขยายตัวของบริการเพิ่มขึ้น และต้นทุนการดำเนินงานต่ำลง จะทำให้การดำเนินงานมีประสิทธิภาพสูงขึ้นในที่สุด

การดำเนินงานอย่างมีประสิทธิภาพ (Operational Efficiency) คือ การเพิ่มประสิทธิภาพเครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล เครือข่าย และทรัพย์สินอื่นๆ ให้เกิดประโยชน์และมีความพร้อมใช้งานสูงสุด นอกจากนี้ การดำเนินงานอย่างมีประสิทธิภาพยังรวมถึงการออกแบบให้มีความสามารถในการรองรับการขยายตัวของบริการเพื่อรองรับการดำเนินงานที่เปลี่ยนแปลงตลอดเวลา ที่สำคัญ ภาครัฐควรต้องให้ความสำคัญต่อการปรับปรุงประสิทธิภาพของโครงสร้างพื้นฐานตาม SLA การประยุกต์ใช้งาน Virtualization และ ระบบคลาวด์ การพัฒนาระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล ระบบจัดเก็บข้อมูลแบบถาวร (Data Archiving) การพัฒนาเพื่อให้เกิดความต่อเนื่องในการดำเนินงาน รวมไปถึงการลงทุนอย่างคุ้มค่า

คุณลักษณะสำคัญสำหรับทิศทางอนาคต

โครงสร้างพื้นฐานสำหรับอนาคตควรปฏิบัติตามมาตรฐานที่ออกแบบมาสำหรับโครงสร้างพื้นฐานในแต่ละมิติ ซึ่งมาตรฐานเหล่านี้เป็นไปตามวิธีปฏิบัติที่เป็นเลิศ (Best Practice) เพื่อเพิ่มประสิทธิภาพการดำเนินงาน

ในแต่ละมิติของโครงสร้างพื้นฐานสำหรับอนาคตจะถูกบริหารจัดการตามระดับประสิทธิภาพการดำเนินงาน หน่วยงานสามารถดำเนินงานในมิติต่างๆ ได้เพื่อบรรลุในระดับประสิทธิภาพที่สูงขึ้น

โครงสร้างพื้นฐานที่มีประสิทธิภาพควรรองรับการบริการที่ยืดหยุ่นและมีต้นทุนการดำเนินงานที่ต่ำลง โครงสร้างพื้นฐานต้องมีความสามารถในการรองรับภารกิจหลักและมีความสามารถในการรองรับการเปลี่ยนแปลงของความต้องการที่อาจเกิดขึ้น

หน่วยงานสามารถคาดการณ์ถึงความพร้อมและความสามารถในการให้บริการของตนได้

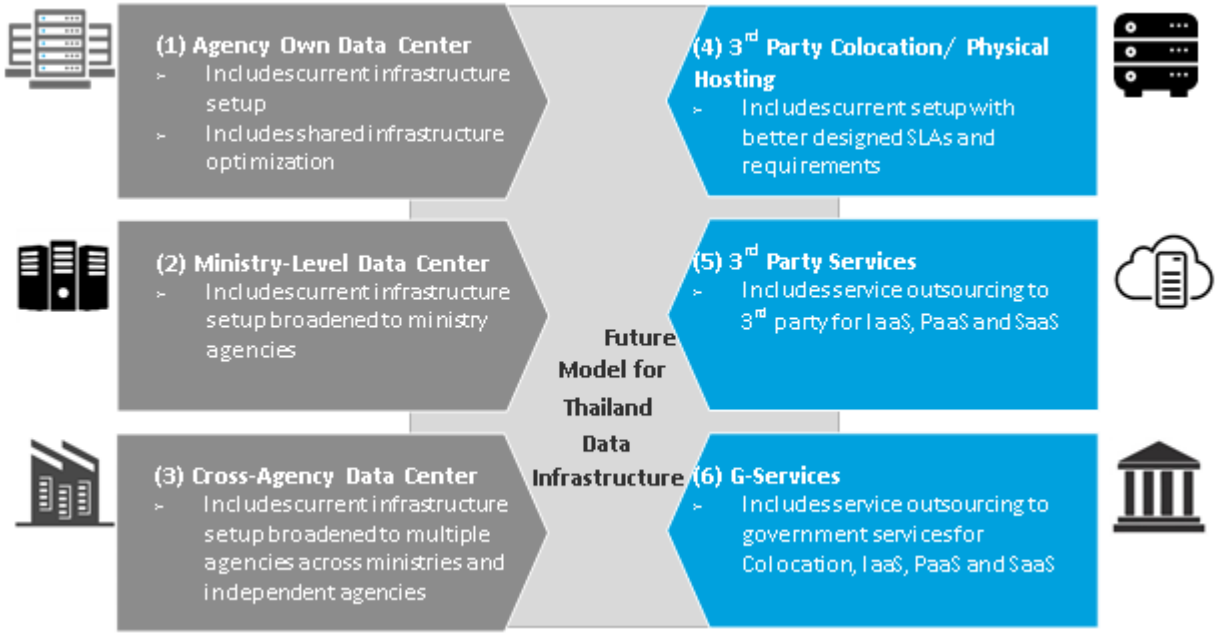
10. รูปแบบการดำเนินงานในอนาคตสำหรับโครงสร้างพื้นฐานด้านข้อมูลของภาครัฐไทย

โครงสร้างพื้นฐานด้านข้อมูลของภาครัฐในอนาคตจะถูกบริหารจัดการภายใต้กรอบการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) ซึ่งภายใต้กรอบการพัฒนานี้มีการกำหนดยุทธศาสตร์ในช่วงระยะ 5 ปี ตั้งแต่ปี ค.ศ. 2018 - 2022 เพื่อให้หน่วยงานต่างๆ ดำเนินการเปลี่ยนผ่านจากการดำเนินงานในรูปแบบเดิมไปสู่การดำเนินงานในรูปแบบใหม่อย่างมีประสิทธิภาพ เพื่อผลักดันให้ประเทศบรรลุเป้าหมายการพัฒนาเศรษฐกิจดิจิทัล และปรับโครงสร้างพื้นฐานให้สอดคล้องกับการดำเนินงานแบบบูรณาการในระยะยาว

ทิศทางการดำเนินงานในอนาคตจำเป็นต้องมีทางเลือกที่หลากหลาย เพื่อให้กระทรวงและหน่วยงานต่างๆ สามารถเลือกใช้เป็นแนวทางดำเนินงานตามความเหมาะสม โดยมีรูปแบบการดำเนินงานในอนาคต (Future Operating Model) สำหรับโครงสร้างพื้นฐานด้านข้อมูลทั้ง 6 รูปแบบ ดังนี้

1) ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center)
2) ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center)
3) ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center)
4) การบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอก (3rd Party Colocation/ Physical Hosting)
5) การบริการโดยหน่วยงานภายนอก (3rd Party Services)
6) การบริการโดยภาครัฐ (G-Services)

หน่วยงานสามารถเลือกใช้แต่ละรูปแบบการดำเนินงานโดยพิจารณาจากสภาวะการปฏิบัติงานในปัจจุบัน โดยรูปแบบการดำเนินงานที่เลือกนั้นควรมีประสิทธิภาพสูงสุดต่อหน่วยงาน



1) ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center)

ศูนย์ข้อมูลประจำหน่วยงานมีรูปแบบการดำเนินงานในอนาคตที่ต่อเนื่องจากศูนย์ข้อมูลของหน่วยงานที่มีอยู่เดิม แต่จำเป็นต้องได้รับการปรับปรุงให้เป็นไปตามมาตรฐานเพื่อรองรับการจัดเก็บข้อมูลที่ต้องการความปลอดภัยสูงและข้อมูลสำคัญของหน่วยงาน ทั้งนี้ ด้วยข้อจำกัดเรื่องงบประมาณและทางเลือกของรูปแบบการดำเนินงานในอนาคตอื่นที่ประหยัดกว่า ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) จึงเหมาะสมสำหรับกรณีที่หน่วยงานมีความจำเป็นเท่านั้น โดยหน่วยงานต้องรายงานอัตราการใช้ประโยชน์ การรักษาความปลอดภัย เหตุผล และวัตถุประสงค์การใช้งาน เมื่อมีการใช้รูปแบบศูนย์ข้อมูลประจำหน่วยงานนี้

คำนิยาม

ศูนย์ข้อมูลประจำหน่วยงานคือ รูปแบบที่มีอยู่เดิมในปัจจุบัน โดยมีการใช้งบประมาณเพื่อลงทุนการก่อสร้างอาคารสถานที่ที่เหมาะสมในการจัดเก็บข้อมูลให้แก่หน่วยงานใดหน่วยงานหนึ่งโดยเฉพาะ และมีระดับการบริการ ความปลอดภัย และการใช้ประโยชน์สูงกว่ารูปแบบอื่นๆ

ศูนย์ข้อมูลประจำหน่วยงานจำเป็นต้องยกระดับให้สอดคล้องกับแนวทางมาตรฐานและระดับคุณสมบัติ (Maturity Level) ตามเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards) ในสภาวะปัจจุบัน หน่วยงานส่วนใหญ่เผชิญกับปัญหาและความท้าทายอันเนื่องมาจากการไม่ได้นำมาตรฐานที่เกี่ยวข้องมาประยุกต์ใช้ เช่น ขาดความยืดหยุ่นในการให้บริการหรือใช้ทรัพยากร ขาดความสามารถในการให้บริการอย่างต่อเนื่อง และขาดการบริหารข้อมูลอย่างเหมาะสม เป็นต้น ซึ่งทั้งหมดนี้ส่งผลให้มีการใช้จ่ายงบประมาณอย่างสิ้นเปลือง

ศูนย์ข้อมูลประจำหน่วยงานในอนาคตจะมุ่งเน้น 4 มิติสำคัญของการพัฒนาโครงสร้างพื้นฐานด้านข้อมูล ดังนี้

จัดการข้อมูลและการประมวลผลที่ต้องการความปลอดภัยสูง	เพิ่มความพร้อมใช้งานและความเสถียรของข้อมูล	ลดต้นทุนการดำเนินงานปัจจุบัน	พัฒนาความพร้อมและความสามารถของทรัพยากรบุคคล

แนวทางการดำเนินงานในอนาคต

- เจ้าหน้าที่ศูนย์ข้อมูลของหน่วยงานในปัจจุบันจะมีหน้าที่จัดการศูนย์ข้อมูลประจำหน่วยงานทั้งหมด
- หน่วยงานจะต้องรายงานข้อมูลเกี่ยวกับประสิทธิภาพของศูนย์ข้อมูล
- เจ้าหน้าที่ศูนย์ข้อมูลของหน่วยงานจะปฏิบัติงานและบำรุงรักษาศูนย์ข้อมูลประเภทนี้ โดยมีการสนับสนุนการฝึกอบรมบุคลากรตามความเชี่ยวชาญ

2) ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center)

ศูนย์ข้อมูลระดับกระทรวงหมายถึง ศูนย์ข้อมูลขนาดใหญ่ที่จะมีการพัฒนาเป็นโครงสร้างพื้นฐานสำคัญในระดับกระทรวง โครงสร้างพื้นฐานประเภทนี้จำเป็นต้องมีความเสถียร ประสิทธิภาพ และสามารถตอบสนองความต้องการในปัจจุบันและอนาคต นอกจากนี้ ศูนย์ข้อมูลระดับกระทรวงต้องมีความสามารถในการรองรับการขยายตัวของบริการ (Scalability) ที่จำเป็นในอนาคต ต้องมีการรักษาความปลอดภัยที่สูง และรองรับความต้องการด้าน IT ของหน่วยงานในสังกัดได้ ดังนั้น ศูนย์ข้อมูลระดับกระทรวงจะมีประสิทธิภาพสูง มุ่งเน้นการให้บริการแก่ประชาชน ครบวงจร เข้าถึงได้ง่าย และคุ้มค่า

คำนิยาม

ศูนย์ข้อมูลระดับกระทรวง คือ ศูนย์ข้อมูลขนาดใหญ่ที่เป็นศูนย์ข้อมูลประจำหน่วยงาน โดยจะมีการพัฒนาเพื่อรองรับการดำเนินงานของทั้งกระทรวงเพื่อจัดเก็บข้อมูล การบริการ และแอปพลิเคชันของหน่วยงานต่างๆ ภายในสังกัดของกระทรวง

ศูนย์ข้อมูลระดับกระทรวง คือ การบริการรูปแบบใหม่ที่ใช้ประโยชน์จากโครงสร้างพื้นฐานที่มีอยู่เดิมในการให้บริการแก่หน่วยงานต่างๆ ในสังกัดกระทรวง ทั้งนี้ ศูนย์ข้อมูลที่มีขนาดใหญ่จะถูกเปลี่ยนเป็นศูนย์ข้อมูลระดับกระทรวงโดยพิจารณาจากขนาดศูนย์ข้อมูล ข้อมูลหน่วยงาน สถานที่ตั้ง และความพร้อมของโครงสร้างพื้นฐานปัจจุบัน นอกจากนี้ ศูนย์ข้อมูลขนาดใหญ่ที่ถูกเปลี่ยนรูปแบบการดำเนินงานนั้นจะถูกยกระดับให้สอดคล้องกับแนวทางมาตรฐานในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards) ซึ่งในปัจจุบัน หน่วยงานที่ใช้ศูนย์ข้อมูลที่มีอยู่เดิมไม่มีการใช้ข้อมูลร่วมกัน ซึ่งในอนาคตศูนย์ข้อมูลระดับกระทรวงจะช่วยให้หน่วยงานในสังกัดกระทรวงเดียวกันสามารถใช้ข้อมูลต่างๆ ร่วมกันได้

ข้อดีของศูนย์ข้อมูลรูปแบบนี้คือ การใช้พื้นที่จัดเก็บข้อมูลนั้นมีการใช้งานอย่างคุ้มค่า (Economies of Scale) ซึ่งเพิ่มระดับการใช้งานพื้นที่จัดเก็บข้อมูล มีโครงสร้างพื้นฐานที่สอดคล้องตามมาตรฐานสำหรับหน่วยงานต่างๆ และมีการรักษาความปลอดภัยของข้อมูลเป็นอย่างดี องค์ประกอบสำคัญของศูนย์ข้อมูลระดับกระทรวงคือสถานที่ตั้ง เนื่องจากหน่วยงานต่างๆ ในสังกัดกระทรวงเดียวกันจำเป็นต้องตั้งอยู่ในพื้นที่ใกล้เคียงกัน นอกจากนี้ ศูนย์ข้อมูลประเภทนี้สามารถจัดเก็บข้อมูลได้หลากหลายซึ่งหน่วยงานในสังกัดกระทรวงเดียวกันสามารถนำมาใช้ประโยชน์ได้ ทั้งนี้ ศูนย์ข้อมูลระดับกระทรวงอาจมีข้อจำกัดคือไม่เหมาะสำหรับการจัดเก็บข้อมูลด้านความมั่นคงของประเทศ

ศูนย์ข้อมูลระดับกระทรวงในอนาคตจะมุ่งเน้น 4 มิติสำคัญของโครงสร้างพื้นฐานด้านข้อมูล ดังนี้

จัดการข้อมูลและการประมวลผลในปริมาณมาก	การประหยัดจากการเพิ่มพื้นที่จัดเก็บข้อมูลช่วยเพิ่มอัตราการใช้งาน	ลดต้นทุนการดำเนินงานของการปฏิบัติงานปัจจุบัน	การบริการแบบมาตรฐานโดยจำแนกข้อมูลอย่างเป็นระบบภายในกระทรวง

แนวทางการดำเนินงานในอนาคต

- เจ้าหน้าที่ระดับกระทรวงประจำการที่ศูนย์ข้อมูลมีหน้าที่จัดการศูนย์ข้อมูลระดับกระทรวงในภาพรวม
- เจ้าหน้าที่ระดับกระทรวงประกอบด้วย เจ้าหน้าที่เดิมของหน่วยงานและเจ้าหน้าที่จากหน่วยงานอื่นในสังกัดกระทรวงเดียวกัน เพื่อจัดตั้งเป็นคณะทำงานชุดใหญ่
- เจ้าหน้าที่เดิมจะปฏิบัติงานและบำรุงรักษา โดยจำนวนของเจ้าหน้าที่สามารถเพิ่มเติมให้สอดคล้องกับความต้องการ
- เจ้าหน้าที่ศูนย์ข้อมูลจะรายงานให้ภาครัฐทราบและจัดทำรายงานเกี่ยวกับประสิทธิภาพศูนย์ข้อมูล อัตราการใช้งาน การจัดการต้นทุน และการจัดการทรัพยากร

3) ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center)

หน่วยงานในสังกัดกระทรวงและหน่วยงานอิสระหลายแห่งเล็งเห็นความสำคัญของศูนย์ข้อมูลแบบบูรณาการที่สามารถจัดเก็บข้อมูลปริมาณมหาศาลอย่างปลอดภัยและที่สามารถใช้พื้นที่จัดเก็บข้อมูลอย่างคุ้มค่า (Economies of Scale) ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) นั้นมีขนาดใหญ่และมีความพร้อมด้านพื้นที่อยู่แล้ว ซึ่งศูนย์ข้อมูลเหล่านี้จะถูกพัฒนาจากการดำเนินงานโดยหน่วยงานเดิมในปัจจุบันไปสู่ผู้ให้บริการโครงสร้างพื้นฐานขนาดใหญ่ที่พึ่งพาตัวเองได้และสามารถดำเนินงานในรูปแบบของศูนย์ข้อมูลภาครัฐ ที่สำคัญ ศูนย์ข้อมูลให้บริการระหว่างหน่วยงานนั้นตอบโจทย์ความต้องการโครงสร้างพื้นฐานทางกายภาพเพื่อเชื่อมโยงหน่วยงานภาครัฐต่างๆ เข้าด้วยกันและรองรับการเชื่อมต่อของข้อมูลระหว่างหน่วยงานได้ในอนาคต

คำนิยาม

ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน คือ ศูนย์ข้อมูลประจำหน่วยงานในปัจจุบันที่มีโครงสร้างพื้นฐานสามารถรองรับการบริการระหว่างหน่วยงานด้วยงบประมาณที่น้อยลง นอกจากนี้ ศูนย์ข้อมูลดังกล่าวยังมีประสิทธิภาพสูง สามารถให้บริการจัดเก็บข้อมูลของหน่วยงานจากกระทรวงและหน่วยงานอิสระต่างๆ ได้อย่างมีประสิทธิภาพ

ปัจจุบันหลายหน่วยงานดำเนินงานศูนย์ข้อมูลของตนเองหรือจัดจ้างหน่วยงานภายนอกในการให้บริการศูนย์ข้อมูล ซึ่งการเพิ่มประสิทธิภาพการใช้ทรัพยากร การดำเนินงาน การรักษาความปลอดภัย และการดำเนินงานภายใต้งบประมาณที่จำกัดนั้นมีความจำเป็นอย่างยิ่ง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) ช่วยให้การแลกเปลี่ยนข้อมูลและความร่วมมือระหว่างหน่วยงานภาครัฐนั้นรวดเร็วขึ้น ศูนย์ข้อมูลลักษณะนี้ให้บริการเครื่องแม่ข่ายกลาง พื้นที่วางเครื่องแม่ข่าย ระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล ระบบเครือข่าย ระบบสื่อสารข้อมูล ระบบรักษาความปลอดภัย ระบบตรวจสอบสถานะ ระบบทำความเย็น ระบบไฟฟ้า ระบบป้องกันอัคคีภัย และการบริการตลอดเวลา 24 ชั่วโมง 7 วันต่อสัปดาห์ เป็นต้น

ศูนย์ข้อมูลให้บริการระหว่างหน่วยงานในอนาคตจะมุ่งเน้น 4 มิติสำคัญของโครงสร้างพื้นฐานด้านข้อมูล ดังนี้

ศูนย์ข้อมูลให้บริการระหว่างหน่วยงานมีพัฒนาการจากศูนย์ข้อมูลในปัจจุบันที่มีพื้นที่และโครงสร้างพื้นฐานด้านข้อมูลขนาดใหญ่ นอกจากนี้ ศูนย์ข้อมูลลักษณะนี้สามารถพัฒนาเพื่อตอบสนองความต้องการอย่างมีประสิทธิภาพ ให้บริการได้อย่างมีคุณภาพ มีความพร้อมใช้งาน ร่วมกับเทคโนโลยีที่เหมาะสม และสามารถรองรับการขยายตัวของบริการในอนาคต

แนวทางการดำเนินงานในอนาคต

- เจ้าหน้าที่ศูนย์ข้อมูลกลางจะถูกจัดตั้งขึ้นเพื่อจัดการดูแลภาพรวมของศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center)
- เจ้าหน้าที่จากศูนย์ข้อมูลของหน่วยงานจะเข้าร่วมเป็นส่วนหนึ่งของเจ้าหน้าที่ศูนย์ข้อมูลกลาง
- เจ้าหน้าที่ศูนย์ข้อมูลกลางจะต้องรายงานข้อมูลสำคัญเกี่ยวกับประสิทธิภาพ การดำเนินงาน และการจัดการศูนย์ข้อมูลให้หน่วยงานกลางทราบ
- เจ้าหน้าที่ศูนย์ข้อมูลเดิมจะมีหน้าที่ปฏิบัติงานและบำรุงรักษาศูนย์ข้อมูล โดยความรับผิดชอบจะครอบคลุมถึงการดำเนินงานศูนย์ข้อมูล โดยภาครัฐจะให้การฝึกอบรมเพื่อความเชี่ยวชาญ

4) การบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอก (3rd Party Colocation/Physical Hosting)

การบริการพื้นที่วางเครื่องแม่ข่าย (3rd Party Colocation) เป็นองค์ประกอบสำคัญของระบบโครงสร้างพื้นฐานด้านข้อมูลและทิศทางในอนาคต นอกจากนี้ หลายหน่วยงานเชื่อว่าการบริการพื้นที่วางเครื่องแม่ข่ายสามารถช่วยลดปัญหาด้านงบประมาณและปัญหาด้านบุคลากรได้ นอกจากนี้ การบริการพื้นที่วางเครื่องแม่ข่ายไม่ใช่ปรากฏการณ์ที่เกิดขึ้นใหม่ แต่หน่วยงานภาครัฐในหลายประเทศและประเทศไทยมีการปฏิบัติที่ประสบผลสำเร็จมาระยะหนึ่งแล้ว “Colocation” หรือ “Colo” หมายถึงการเช่าพื้นที่วางเครื่องแม่ข่ายและฮาร์ดแวร์ประมวลผลโดยได้รับการบริการโครงสร้างพื้นฐานอื่นๆ ร่วมด้วย เช่น อาคารและสถานที่ ไฟฟ้า ระบบทำความเย็น การเชื่อมต่อเครือข่าย และความปลอดภัยทางกายภาพ โดยที่หน่วยงานเองเป็นผู้จัดหาเครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล และการบำรุงรักษาเองในบางกรณี

ในอนาคต การบริการพื้นที่วางเครื่องแม่ข่าย (3rd Party Colocation) จะไม่เปลี่ยนแปลงไปจากปัจจุบันมาก เว้นแต่ SLA ที่อาจเปลี่ยนแปลงตามความเหมาะสมในแต่ละราย ที่สำคัญ ประเภทข้อมูลที่เหมาะสมสำหรับการบริการพื้นที่วางเครื่องแม่ข่ายคือข้อมูลทั่วไปซึ่งอาจเป็นข้อมูลสาธารณะ

คำนิยาม

การบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอกคือ การใช้บริการหน่วยงานภายนอกในการจัดการและให้บริการโครงสร้างพื้นฐานเพื่อรองรับการจัดเก็บเครื่องแม่ข่ายของหน่วยงานในสภาพแวดล้อมที่มีประสิทธิภาพ ที่สามารถรองรับการเชื่อมต่อ ที่มีการรักษาความปลอดภัย ที่มีเสถียรภาพ ลดค่าใช้จ่าย CAPEX และ OPEX ได้ นอกจากนี้ การบริการพื้นที่วางเครื่องแม่ข่ายสามารถจัดเก็บข้อมูลที่สำคัญต่อพันธกิจ (Mission Critical Data) ที่ต้องการการดูแลอย่างมีประสิทธิภาพและพร้อมใช้งานเสมอ

ในปัจจุบัน หน่วยงานหลายแห่งใช้การบริการพื้นที่วางเครื่องแม่ข่ายเพื่อตอบสนองความต้องการพื้นที่ศูนย์ข้อมูล ผู้ให้บริการพื้นที่วางเครื่องแม่ข่ายมีความเชี่ยวชาญและสามารถติดตามสถานะของการบริการได้ตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์โดยใช้แนวทางปฏิบัติของภาครัฐเป็นกรอบในการให้บริการ นอกจากนี้ การบริการพื้นที่วางเครื่องแม่ข่ายสามารถรองรับข้อมูลสำคัญและความต้องการด้าน IT สามารถจัดเก็บข้อมูลในศูนย์ข้อมูลที่มีระบบสำรองและความปลอดภัย และสามารถรองรับการขยายตัวของบริการอย่างมีประสิทธิภาพ โดยที่ระบบ IT ของหน่วยงาน เว็บไซต์ และแอปพลิเคชันถูกจัดเก็บไว้โดยมีระบบรักษาความปลอดภัยกายภาพที่ทันสมัย ซึ่งช่วยลดค่าใช้จ่ายในการจ้างเจ้าหน้าที่รักษาความปลอดภัย

การบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอกในอนาคตจะมุ่งเน้น 4 มิติสำคัญของโครงสร้างพื้นฐานด้านข้อมูลดังนี้

เพิ่มความสามารถรองรับการขยายตัวของบริการโดยมีโครงสร้างพื้นฐานพร้อมใช้งาน	การเชื่อมต่อดีขึ้น และมีการเชื่อมต่อเครือข่ายสำรอง	ติดตามสถานะและช่วยเหลือตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์	ลดค่าใช้จ่ายภาครัฐสำหรับความต้องการศูนย์ข้อมูลขนาดเล็ก

การบริการพื้นที่วางเครื่องแม่ข่ายจะถูกพัฒนาจากรูปแบบในปัจจุบันด้วยการกำหนด SLA ให้ผู้ให้บริการปฏิบัติตามโดยหน่วยงานจะเลือกผู้ให้บริการพื้นที่วางเครื่องแม่ข่ายอย่างเหมาะสม โดยมีแนวทางตามเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards) สำหรับการบริการพื้นที่วางเครื่องแม่ข่ายนี้ หน่วยงานจำเป็นต้องเลือกประเภทข้อมูลที่เหมาะสมสำหรับการใช้บริการพื้นที่วางเครื่องแม่ข่ายอย่างรอบคอบ

แนวทางการดำเนินงานในอนาคต

- หน่วยงานที่ใช้บริการพื้นที่วางเครื่องแม่ข่ายจะมีหน้าที่บริหารความสัมพันธ์กับผู้ให้บริการ ดูแลรักษา และจัดการข้อมูลทั้งหมด
- ภาครัฐจะต้องจัดทำรายละเอียดเกี่ยวกับราคา ข้อตกลงระดับการให้บริการ (SLA) และแนวทางปฏิบัติสำหรับผู้ให้บริการ ซึ่งจะเผยแพร่ให้แก่หน่วยงานต่างๆ ต่อไป
- ผู้ให้บริการจะต้องให้บริการตามที่ระบุในสัญญาอย่างเคร่งครัด

5) การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS)

การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) นั้นเป็นการให้บริการในรูปแบบ On-demand ซึ่งมีความสำคัญและได้รับความนิยมมากขึ้น การบริการโดยหน่วยงานภายนอกสามารถช่วยให้หน่วยงานภาครัฐลดต้นทุนด้านโครงสร้างพื้นฐาน ลดปัญหาด้านบุคคลกร และลดความจำกัดในด้านเทคโนโลยีของหน่วยงานเอง เนื่องจากความต้องการดังล่าวจะถูกรับผิดชอบและให้บริการโดยหน่วยงานภายนอก นอกจากนี้ หลายหน่วยงานเชื่อว่าการย้ายไปใช้การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) นี้จะช่วยประหยัดต้นทุนการจัดซื้อเครื่องแม่ข่าย ลดค่าใช้จ่ายการบำรุงรักษาและค่าใช้จ่ายด้านบุคลากรอย่างมหาศาล ซึ่งการบริการโดยหน่วยงานภายนอกมีความเสถียร ความโปร่งใส และความสามารถให้การบริการได้ตาม SLA ที่กำหนด การนำระบบคลาวด์ IaaS, PaaS และ SaaS มาใช้นั้นจะส่งผลให้หน่วยงานต่างๆ ลดอัตราการปล่อยก๊าซเรือนกระจกอย่างมหาศาล เพิ่มประสิทธิภาพ ลดความเสี่ยง และลดต้นทุนได้ หากมองในเชิงเศรษฐกิจ ระบบคลาวด์เอื้อให้หน่วยงานภาครัฐต่างๆ สามารถปรับปรุงการดำเนินงานให้สอดคล้องกับความต้องการของภาคประชาชนและธุรกิจ สามารถรองรับการขยายตัวของบริการ และตอบสนองได้อย่างรวดเร็ว ที่สำคัญ การปฏิบัติงานในอนาคตของการให้บริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) จะสามารถรองรับข้อมูลทั่วไปที่มีขนาดใหญ่ที่ต้องมีความพร้อมใช้งานสูง (High Availability)

คำนิยาม

การบริการโดยหน่วยงานภายนอก (3rd Party Services) หมายรวมถึงการบริการคลาวด์ในรูปแบบ IaaS, PaaS และ SaaS ซึ่งให้บริการโดยภาคเอกชนที่หน่วยงานภาครัฐสามารถจัดเก็บข้อมูลประเภทที่เหมาะสมไว้บนระบบโดยไม่ต้องมีโครงสร้างพื้นฐานทางกายภาพหรือระบบจัดเก็บข้อมูลเอง ความรับผิดชอบด้านการดำเนินงานและอุปกรณ์ เช่น เครื่องแม่ข่าย ระบบจัดเก็บข้อมูล และโครงสร้างพื้นฐานต่างๆ ถือเป็นความรับผิดชอบของหน่วยงานภาคเอกชนที่ให้บริการ นอกจากนี้ การให้บริการลักษณะดังกล่าวยังมีต้นทุนที่เหมาะสม มีประสิทธิภาพ สามารถรองรับการขยายตัวของบริการ และมีประสิทธิภาพในการใช้พลังงานเป็นอย่างดี

การใช้การบริการโดยหน่วยงานภายนอก (3rd Party Services) จะปรับเปลี่ยนรูปแบบการใช้ข้อมูลและการใช้การบริการซึ่งส่งผลให้หน่วยงานภาครัฐสามารถเพิ่มประสิทธิภาพการดำเนินงาน เพิ่มความคล่องตัว ลดความยุ่งยาก ลดต้นทุนด้านพลังงานและทรัพยากร นอกจากนี้ ระบบคลาวด์นี้ยังอำนวยความสะดวกให้หน่วยงานภาครัฐต่างๆ สามารถใช้บริการในลักษณะ On-demand ซึ่งมีความยืดหยุ่นในกรณีที่ความต้องการเพิ่มขึ้นหรือลดลง โดยไม่จำเป็นต้องจัดเตรียมทรัพยากรใดๆ

การบริการโดยหน่วยงานภายนอกในอนาคตจะมุ่งเน้น 4 มิติสำคัญของโครงสร้างพื้นฐานด้านข้อมูล ดังนี้

- ลดต้นทุน CAPEX และ OPEX
- มีความคล่องตัวของพื้นที่จัดเก็บข้อมูลและการย้ายภาระงาน (Workload Migration)
- มีความคล่องตัวและรวดเร็วในการจัดซื้อและประหยัดงบประมาณ
- เพิ่มประสิทธิภาพเนื่องจากประหยัดในการเพิ่มพื้นที่จัดเก็บข้อมูล (Economies of Scale)

การบริการโดยหน่วยงานภายนอก (3rd Party Services) จะเป็นที่ยอมรับมากขึ้น โดยเป็นการพัฒนาจากรูปแบบปัจจุบันไปสู่การให้บริการด้วยต้นทุนที่ต่ำลงและมีการประยุกต์ใช้เทคโนโลยีใหม่ในอนาคต นอกจากนี้ ทิศทางในอนาคตของการบริการโดยหน่วยงานภายนอกจำเป็นต้องปฏิบัติตามมาตรฐานและ SLA ที่ภาครัฐกำหนด โดยหน่วยงานจะได้รับคำแนะนำในการจัดจ้างผู้ให้บริการที่เหมาะสมและในการเลือกข้อมูลที่เหมาะสมมาจัดเก็บไว้บนระบบคลาวด์อีกด้วย

แนวทางการดำเนินงานในอนาคต

- หน่วยงานภาครัฐที่ใช้บริการหน่วยงานภายนอกจะมีหน้าที่บริหารความสัมพันธ์กับผู้ให้บริการและจัดเตรียมข้อมูลทั้งหมด
- ภาครัฐจะจัดทำรายละเอียดด้านราคา ข้อตกลงระดับการให้บริการ (SLA) และแนวทางปฏิบัติสำหรับผู้ให้บริการซึ่งจะเผยแพร่ให้แก่หน่วยงานต่างๆ ต่อไป
- ผู้ให้บริการจะต้องให้บริการตามที่ระบุในสัญญาอย่างเคร่งครัด

6) การบริการโดยภาครัฐ (G-Services: Colocation, IaaS, PaaS และ SaaS)

หน่วยงานภาครัฐต่างระบุว่า การบริการโดยภาครัฐ (G-Services: Colocation, IaaS, PaaS และ SaaS) เป็นหนึ่งในรูปแบบการดำเนินงานที่มีศักยภาพสูงสุดที่ให้หน่วยงานภาครัฐสามารถปฏิบัติงานภายใต้การบริการที่มีความปลอดภัยสูงซึ่งดูแลโดยภาครัฐเอง นอกจากนี้ หน่วยงานยังเชื่อว่าการบริการโดยภาครัฐนั้นจะเป็นอนาคตของการพัฒนาศูนย์ข้อมูลและยังจัดลำดับความสำคัญไว้เป็นอันดับแรกสุดเนื่องจากมีการบูรณาการและบริหารจัดการโดยภาครัฐเอง นอกจากนี้ การบริการโดยภาครัฐนั้นจะลดค่าใช้จ่ายการลงทุน ลดค่าใช้จ่ายการดำเนินงาน ลดภาระการบำรุงรักษา สามารถจัดเก็บข้อมูลสำคัญ และมีความปลอดภัยสูงซึ่งเป็นการลดภาระของภาครัฐในภาพรวม ดังนั้น การเปลี่ยนไปใช้การบริการโดยภาครัฐ (G-Services) จะช่วยประหยัดงบประมาณการจัดซื้อเครื่องแม่ข่ายและการดูแลรักษาได้อย่างมหาศาล รูปแบบการดำเนินการในอนาคตของการบริการโดยภาครัฐจะครอบคลุมการบริการ เช่น Colocation, IaaS, PaaS และ SaaS ภายใต้การบริการนี้ภาครัฐสามารถแก้ไขและลดข้อจำกัดด้านความสามารถของบุคลากรเพื่อลดปัญหาในการดูแลรักษาได้อย่างดี นอกจากนี้ การบริการดังกล่าวยังรวมถึงคำแนะนำจากผู้เชี่ยวชาญและการโอนความเสี่ยงการดำเนินงานศูนย์ข้อมูลไปยังผู้เชี่ยวชาญที่ดูแลระบบการบริการ G-Services นี้

อย่างไรก็ตาม บางหน่วยงานโต้แย้งว่าการบริการโดยภาครัฐนั้นเหมาะสำหรับการจัดเก็บข้อมูลทั่วไปเท่านั้น เช่น ระบบสารบรรณอิเล็กทรอนิกส์ ไปรษณีย์อิเล็กทรอนิกส์ และข้อมูลที่เผยแพร่ต่อสาธารณะ ดังนั้นจึงจำเป็นที่ภาครัฐเองต้องทำให้มั่นใจว่าการบริการโดยภาครัฐนั้นมีโครงสร้างพื้นฐานมีประสิทธิภาพ มีความสามารถรองรับการขยายตัวของบริการ มีความทันสมัยทางเทคโนโลยี และมีความปลอดภัยเพื่อแก้ไขข้อโต้แย้งเหล่านั้น นอกจากนี้ ข้อได้เปรียบอย่างชัดเจนของการบริการโดยภาครัฐ (G-Services) ที่เหนือกว่าการบริการโดยหน่วยงานภายนอก (3rd Party Services) และการบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอก (3rd Party Colocation) คือมาตรฐานการจัดการความปลอดภัยที่สูงกว่า เนื่องจากการบริการโดยภาครัฐ (G-Services) นี้มีการบริหารงานและจัดเก็บข้อมูลโดยภาครัฐเองซึ่งลดความเสี่ยงต่อข้อมูลสูญหายหรือประเด็นด้านความปลอดภัยสารสนเทศ (Cyber Security) นอกจากนี้ การบริการโดยภาครัฐยังต้องมีการปฏิบัติตาม SLA และให้การช่วยเหลือตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์

คำนิยาม

การบริการโดยภาครัฐ (G-Services) คือ การบริการ Colocation, IaaS, PaaS และ SaaS ที่จัดเตรียมโดยภาครัฐเพื่อให้บริการการจัดการข้อมูล การประมวลผล และการจัดเก็บข้อมูลแก่หน่วยงานภาครัฐในรูปแบบเดียวกับการให้บริการโดยหน่วยงานภายนอกและมีคุณภาพใกล้เคียงกัน แต่การบริการโดยภาครัฐนั้นมีการจัดการความปลอดภัยที่สูงกว่า นอกจากนี้ ทรัพย์สิน เช่น เครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล และอุปกรณ์สนับสนุนอื่นๆ จะอยู่ในความรับผิดชอบของ G-Services โดยประโยชน์ต่างๆ ที่หน่วยงานได้รับคือ ความปลอดภัย ต้นทุนต่ำ มีประสิทธิภาพ สามารถรองรับการขยายตัวของบริการ การใช้พลังงานและงบประมาณอย่างมีประสิทธิภาพ

การบริการโดยภาครัฐ (G-Services) สามารถตอบโจทย์ความต้องการในการรองรับปริมาณข้อมูลที่เพิ่มขึ้นภายใต้งบประมาณที่จำกัด โดยมีการรักษาความปลอดภัยข้อมูล การบูรณาการข้อมูล ระบบช่วยเหลือ มีความคล่องตัว และการประยุกต์ใช้มาตรฐานระดับสูง นอกจากนี้ ทิศทางในอนาคตของการบริการโดยภาครัฐนั้นจะมีการนำมาตรฐานและมีการประยุกต์ใช้การรักษาความปลอดภัยที่เทียบเท่าหรือดีกว่าที่ได้รับจากการบริการโดยหน่วยงานภายนอก

การบริการโดยภาครัฐในอนาคตจะมุ่งเน้น 4 มิติสำคัญของโครงสร้างพื้นฐานด้านข้อมูล ดังนี้

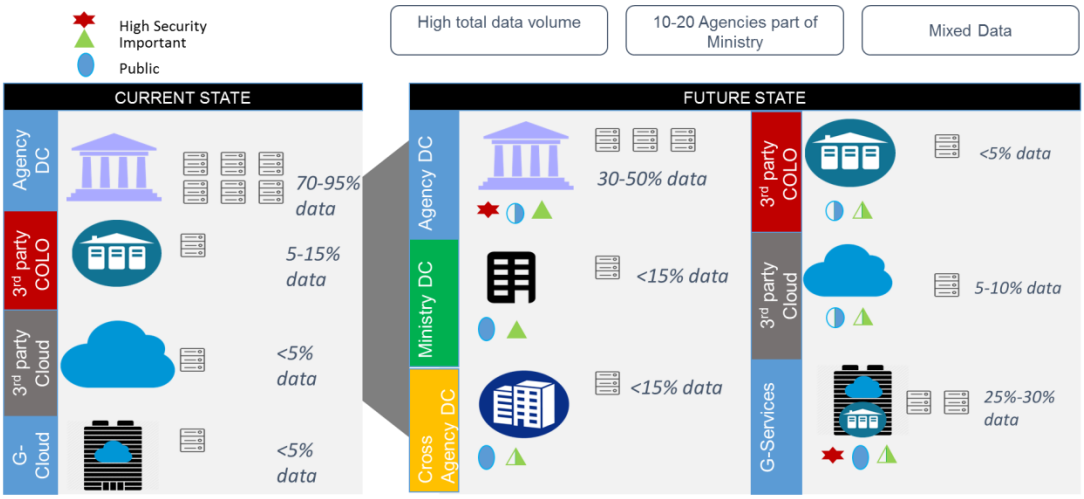
เอื้อให้โครงสร้างพื้นฐานพร้อมรองรับข้อมูลที่ต้องการความปลอดภัยสูง	ลดต้นทุนในการดำเนินงานและต้นทุนสำหรับหน่วยงาน	รองรับการขยายตัวของบริการและเพิ่มประสิทธิภาพในการจัดซื้อจัดหา การจัดการกรอบเวลาและงบประมาณ	เพิ่มประสิทธิภาพและสามารถรองรับการขยายตัวของบริการ

หน่วยงานต่างๆ จะเปลี่ยนไปใช้การบริการโดยภาครัฐ (G-Services) มากขึ้นเรื่อยๆ เพราะประโยชน์จากการให้บริการโดยภาครัฐ มิติสำคัญที่ต้องมุ่งเน้น คือ การบูรณาการข้อมูล/การจำแนกประเภทข้อมูลที่จัดเก็บไว้ การจัดเตรียมบริการแบบ 24 ชั่วโมง 7 วันต่อสัปดาห์ เพื่อช่วยเหลือและเสนอแนะแนวทางแก้ไขปัญหา การฟื้นฟูสภาพและความสามารถในการรองรับการขยายตัวของบริการ เพื่อยกระดับการดำเนินงานที่เป็นมาตรฐานด้วยต้นทุนทั้งหมดที่ต่ำลงสำหรับหน่วยงาน

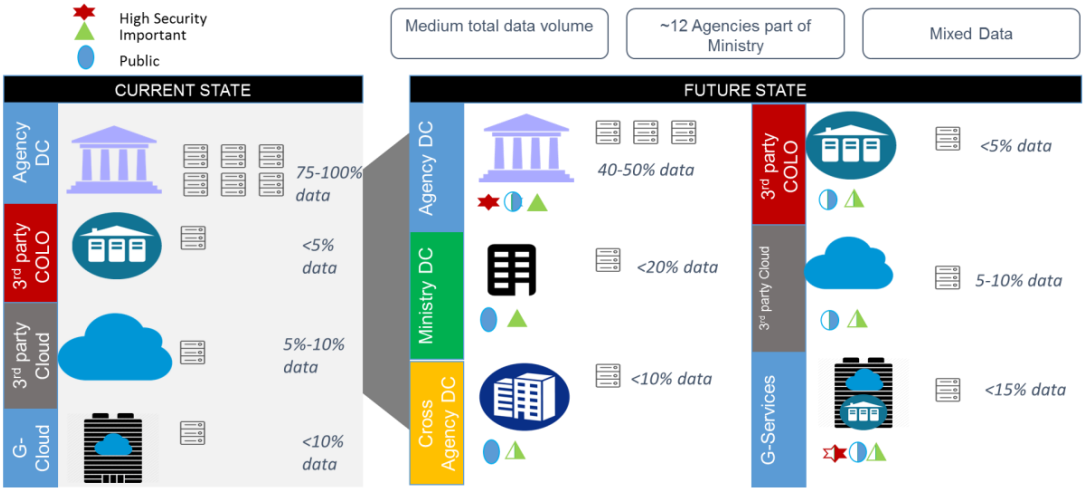
แนวทางการดำเนินงานในอนาคต

- เจ้าหน้าที่ที่จะดำเนินงานการบริการโดยภาครัฐจะเป็นเจ้าหน้าที่ชุดปัจจุบันที่ได้รับการพัฒนาความสามารถที่สูงขึ้นและจะมีการเพิ่มจำนวนเจ้าหน้าที่มากขึ้นหากจำเป็น
- เจ้าหน้าที่ของหน่วยงานจะประสานงานระหว่างหน่วยงานของตนและ G-Services ในรูปแบบของลูกค้าและผู้ให้บริการ อีกทั้งยังสามารถค้นหาข้อมูลเกี่ยวกับการให้บริการและการปฏิบัติตามมาตรฐานได้ เป็นต้น
- ภาครัฐจะจัดทำรายละเอียดด้านราคาและจัดความพร้อมให้บริการแก่ทุกหน่วยงาน

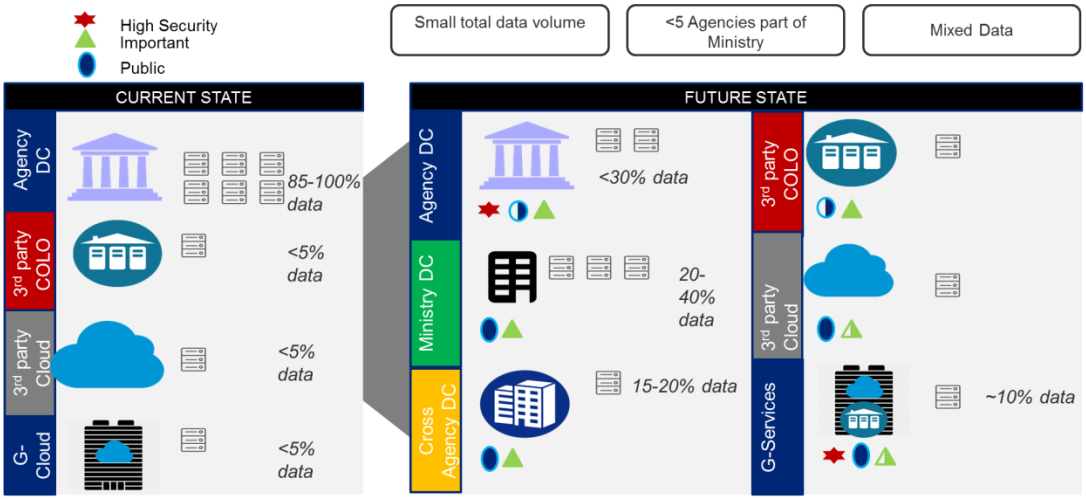
ตัวอย่างแนวทางการจัดเก็บข้อมูลในอนาคตสำหรับกระทรวงที่มีปริมาณข้อมูลมาก



ตัวอย่าง แนวทางการจัดเก็บข้อมูลในอนาคต สำหรับกระทรวงที่มีปริมาณข้อมูลปานกลาง



ตัวอย่าง แนวทางการจัดเก็บข้อมูลในอนาคต สำหรับกระทรวงที่มีปริมาณข้อมูลน้อย



11. ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization Strategy หรือ GDCM Strategy) อยู่บนพื้นฐานความเข้าใจและการวิเคราะห์โครงสร้างพื้นฐานด้านข้อมูลของประเทศไทยอย่างลึกซึ้งและรอบด้าน เช่น โครงสร้างพื้นฐานกายภาพ แอปพลิเคชัน การจัดตั้งศูนย์ข้อมูล มุมมองของเจ้าหน้าที่ภาครัฐ และวิธีปฏิบัติที่เป็นเลิศ (Best Practice) ในระดับสากล รายละเอียดจากการวิเคราะห์ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM Strategy) สามารถทำให้เข้าใจถึงแนวโน้มและความต้องการของประเทศ ความคาดหวังจากหน่วยงานภาครัฐ ประเด็นและปัญหาที่หน่วยงานภาครัฐและภาคประชาชนเผชิญ รวมถึงผลกระทบต่างๆ ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM Strategy) จะก่อให้เกิดประโยชน์มากมาย เช่น การเพิ่มประสิทธิภาพการรักษาความปลอดภัยข้อมูลภาครัฐ การมีบริการที่มีประสิทธิภาพ การประหยัดงบประมาณ การโอนหน้าที่ความรับผิดชอบบางส่วนไปสู่หน่วยงานอื่นที่สามารถดำเนินการได้อย่างมีประสิทธิภาพมากกว่า การลดปัญหาด้านบุคลากร และการยกระดับเทคโนโลยีโครงสร้างพื้นฐานด้านข้อมูลภาครัฐของประเทศไทย

โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) มุ่งเน้นการแก้ไขปัญหาและการลดประเด็นความท้าทายที่หน่วยงานภาครัฐเผชิญดังต่อไปนี้

เพิ่มประสิทธิภาพต้นทุนการดำเนินงานและการบำรุงรักษา

ประเด็นที่สำคัญสำหรับหน่วยงานคือ ต้นทุนที่เพิ่มขึ้นและงบประมาณที่จำกัดเพื่อรองรับความต้องการการบริการ การพัฒนาศูนย์ข้อมูลภาครัฐมีการวางแผนเพื่อลดภาระความรับผิดชอบของหน่วยงานที่ต้องดำเนินงานและบำรุงรักษาโครงสร้างพื้นฐานของตนที่อาจสิ้นเปลืองเกินความจำเป็น

เพิ่มประสิทธิภาพการใช้จ่ายงบประมาณภาครัฐ

ในฐานะที่เป็นส่วนหนึ่งของแผนพัฒนาเศรษฐกิจดิจิทัล การพัฒนาศูนย์ข้อมูลภาครัฐเอื้อให้ภาครัฐสามารถดำเนินงานตามพันธกิจได้อย่างมีประสิทธิภาพด้วยค่าใช้จ่ายที่ลดลง โดยอาศัยประโยชน์จากเทคโนโลยีที่ทันสมัย กรอบแนวคิด และกรอบการทำงาน ซึ่งทั้งหมดที่กล่าวมานี้คือหนึ่งในเป้าหมายหลักของการพัฒนาศูนย์ข้อมูลภาครัฐที่สำคัญ

เพิ่มประสิทธิภาพโครงสร้างพื้นฐานศูนย์ข้อมูล

เมื่อดำเนินการแล้วเสร็จ การกำหนดมาตรฐานจะส่งผลให้ระบบศูนย์ข้อมูล (Data Center Ecosystem) มีประสิทธิภาพ ขณะเดียวกัน การใช้ทรัพยากรร่วมกันจะเพิ่มประสิทธิภาพการใช้งานโครงสร้างพื้นฐานในภาพรวม

พร้อมรองรับความต้องการในอนาคต

ภาครัฐสามารถวางแผนล่วงหน้าเพื่อรับมือความท้าทายในอนาคตได้ เช่น ปริมาณข้อมูลที่เพิ่มขึ้น ความซับซ้อนของข้อมูลที่มากขึ้น และความต้องการของประชาชนที่มากขึ้น ที่สำคัญ หน่วยงานภาครัฐจำเป็นต้องอาศัยแนวคิดเพื่อให้ประชาชนเป็นศูนย์กลาง (Citizen Centricity) โดยดำเนินงานแบบครบวงจร ใช้ประโยชน์จากระบบคลาวด์ ใช้เทคโนโลยีทันสมัยที่มีประสิทธิภาพและทันต่อเหตุการณ์สำหรับปัจจุบันและอนาคต

หน่วยงานมีทางเลือกที่หลากหลาย รวมถึงระบบคลาวด์

หน่วยงานสามารถเลือกทางเลือกที่เหมาะสมที่สุด เช่น การใช้ระบบคลาวด์ ในการยกระดับความน่าเชื่อถือของศูนย์ข้อมูลของตน รวมถึงการจัดเก็บข้อมูลในรูปแบบการดำเนินงานในอนาคตอื่นๆ ทั้ง 6 รูปแบบเพื่อแก้ไขปัญหาของหน่วยงาน

วัตถุประสงค์ของโครงการพัฒนาศูนย์ข้อมูลภาครัฐ

เป้าหมายหลักของโครงการพัฒนาศูนย์ข้อมูลภาครัฐคือ การยกระดับโครงสร้างพื้นฐานด้านข้อมูลให้สอดคล้องกับแผนพัฒนาเศรษฐกิจดิจิทัล เพื่อให้เกิดความยั่งยืน เกิดประสิทธิภาพด้านต้นทุน เกิดนวัตกรรมเทคโนโลยี และเกิดการเตรียมความพร้อมรองรับการการปฏิวัติด้านข้อมูล

วิสัยทัศน์ของโครงการพัฒนาศูนย์ข้อมูลภาครัฐ

วิสัยทัศน์ของโครงการพัฒนาศูนย์ข้อมูลภาครัฐคือ “เพื่อเป็นโครงสร้างพื้นฐานข้อมูลภาครัฐที่ส่งเสริมให้การให้บริการแก่สาธารณะประสบผลสำเร็จ โดยผ่านการดำเนินงานที่มีประสิทธิภาพ ปลอดภัย คุ้มค่า และเหมาะสมที่สุด”

โครงการพัฒนาศูนย์ข้อมูลภาครัฐผลักดันเป้าหมายสำคัญดังต่อไปนี้

- ปรับทิศทางข้อมูลภาครัฐให้สอดคล้องกับคุณลักษณะด้านความปลอดภัยข้อมูล เพื่อเพิ่มการรักษาความปลอดภัยสำหรับข้อมูลด้านความมั่นคงของประเทศ (National Security Data) และมีการจัดการข้อมูลสำคัญ (Important Data) อย่างเหมาะสม
- สนับสนุนโครงสร้างพื้นฐานด้วยแนวทางปฏิบัติและการส่งมอบบริการที่เป็นมาตรฐาน
- เพิ่มประสิทธิภาพด้านต้นทุนและการลงทุนโครงสร้างพื้นฐาน
- ดำเนินการการทำงานร่วมกันทั้งในระดับภาครัฐ กระทรวง หน่วยงาน และภาคเอกชน
- ยกระดับประสิทธิภาพของหน่วยงาน

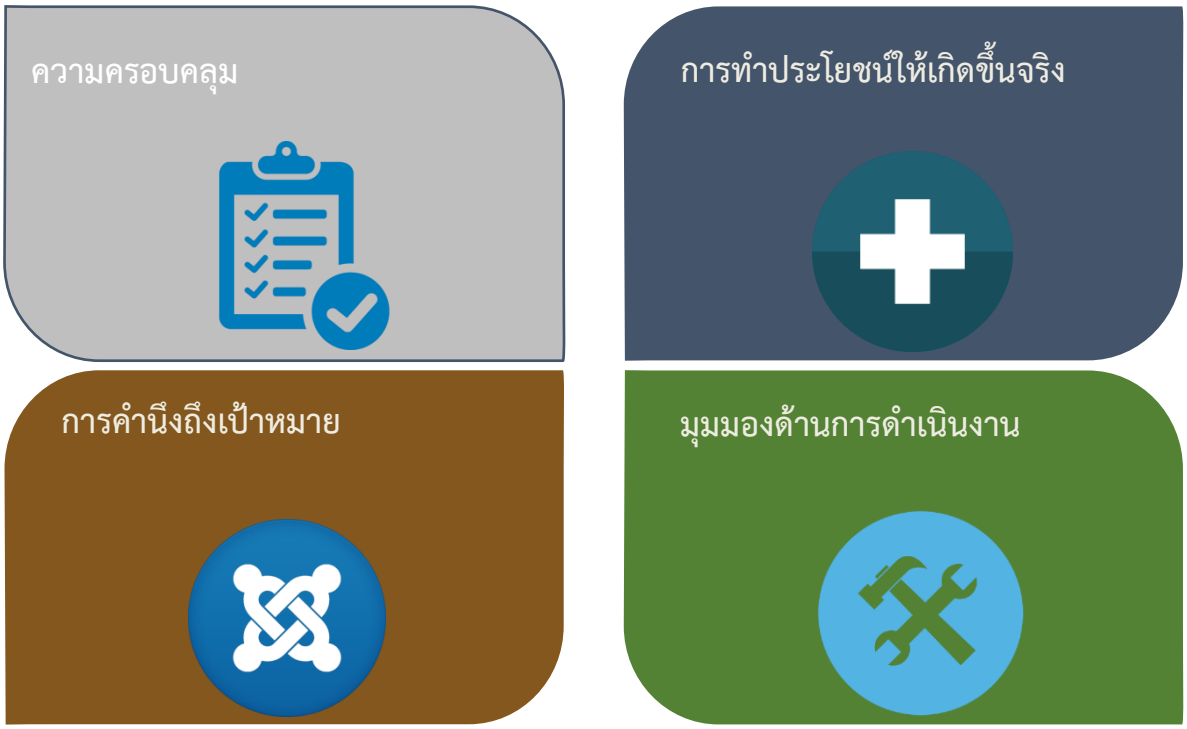
หลักการสำหรับการกำหนดยุทธศาสตร์

การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) วางแผนที่จะนำเทคโนโลยีและแนวทางปฏิบัติสมัยใหม่มาใช้ เพื่อยกระดับสถานะด้านความปลอดภัยของภาครัฐและในขณะเดียวกันยังเอื้อให้เกิดการใช้งานโครงสร้างพื้นฐานด้าน ICT ของภาครัฐอย่างมีประสิทธิภาพ ยุทธศาสตร์นี้จะสนับสนุนภาครัฐและหน่วยงานต่างๆ ในการนำวิธีปฏิบัติที่เป็นเลิศ (Best Practice) มาใช้ให้เกิดประโยชน์อย่างเป็นรูปธรรมและนำไปสู่การสร้างประโยชน์ต่างๆ ที่จะทำให้โครงสร้างพื้นฐานของประเทศเติบโตและยั่งยืน หลักการต่อไปนี้เป็นแนวทางสำคัญในการกำหนดยุทธศาสตร์และการดำเนินงาน

1. **การปรับโครงสร้างพื้นฐานและการพัฒนาภาครัฐให้สอดรับกับแผนพัฒนาเศรษฐกิจดิจิทัล และวิสัยทัศน์ของภาครัฐ**
2. **การใช้ยุทธศาสตร์มุ่งเน้นความปลอดภัยข้อมูล ความสำคัญของแอปพลิเคชัน มุมมองการดำเนินงานในปัจจุบัน และการเติบโต**
3. **การใช้ประโยชน์จากความก้าวหน้าทางเทคโนโลยีที่สำคัญ โดยการนำมาตรฐานและ SLA มาใช้กับรูปแบบการดำเนินงานในอนาคตที่เลือก เพื่อสร้างประโยชน์อย่างเป็นรูปธรรม**
4. **การพิจารณาชุดทักษะ การพัฒนาบุคลากร ความพร้อมของทุนมนุษย์ และการถ่ายทอดทางเทคโนโลยี**
5. **ความรับผิดชอบของหน่วยงานและกระทรวงต่างๆ ในแต่ละขั้นเพื่อผลักดันให้วัตถุประสงค์ในภาพรวมเกิดขึ้นอย่างเป็นรูปธรรม**

คุณลักษณะสำคัญของยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐของประเทศไทย

การพัฒนาและการควบรวมศูนย์ข้อมูล (Data Center Modernization and Data Center Consolidation) เป็นการเพิ่มประสิทธิภาพโครงสร้างพื้นฐานด้านข้อมูลที่มีอยู่เดิม และเป็นการรองรับแอปพลิเคชันที่มีความสำคัญและที่ต้องการความปลอดภัย (Mission-Critical and High-Security Application) การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) เป็นโครงการในระยะยาวที่มุ่งใช้ประโยชน์จากโอกาสใหม่ๆ หรือจากการพัฒนาปรับปรุง เพื่อเพิ่มประสิทธิภาพให้โครงสร้างพื้นฐานนั้นมีความเสถียร มีความพร้อมใช้งาน และมีความปลอดภัยมากขึ้น นอกจากนี้ คุณลักษณะสำคัญที่เอื้อต่อการดำเนินยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐให้ประสบผลสำเร็จนั้นประกอบด้วย



ความครอบคลุม (Comprehensiveness)	• ยุทธศาสตร์ควรมีการตรวจสอบความก้าวหน้าหรือตัวชี้วัด เพื่อบ่งชี้ประโยชน์ที่เกิดขึ้น และทำการวิเคราะห์หาสาเหตุเมื่อเกิดปัญหา
	• ควรมีการระบุความเสี่ยงตั้งแต่เริ่มต้นจนสิ้นสุดการดำเนินงาน
	• ยุทธศาสตร์ต้องสามารถทำให้เกิดความมั่นใจได้ว่า แอปพลิเคชันต่างๆ จะไม่ได้รับผลกระทบจากการหยุดให้บริการ (Downtime) เป็นระยะเวลานาน หากมีการปรับเปลี่ยนยุทธศาสตร์
	• ยุทธศาสตร์ต้องมีแนวทางให้กระทรวงและหน่วยงานสามารถเข้าถึงทางเลือกต่างๆ เพื่อให้การบริการแก่ประชาชนเป็นไปอย่างราบรื่น

การทำประโยชน์ให้เกิดขึ้นจริง (Benefit Realization)	• ยุทธศาสตร์ต้องส่งเสริมวัตถุประสงค์ของโครงการในภาพรวม
	• ยุทธศาสตร์ต้องไม่สร้างความเสียหายต่อภาระงานที่สำคัญต่อพันธกิจ (Mission Critical Workload) อันถือเป็นพื้นฐานสำคัญของการปฏิบัติงาน
	• ยุทธศาสตร์ต้องคำนึงถึงการขยายตัวของการดำเนินงานควบคู่ไปกับการเติบโตของอุตสาหกรรมดิจิทัล การนำเทคโนโลยีมาใช้ และการเพิ่มปริมาณของข้อมูล

การคำนึงถึงเป้าหมาย (End in mind)	• ยุทธศาสตร์ต้องยกระดับการมีประชาชนเป็นศูนย์กลาง (Citizen Centricity)
	• ยุทธศาสตร์ต้องใช้ประโยชน์จากรูปแบบการดำเนินงานที่มีประสิทธิภาพ เพื่อเพิ่มประสิทธิภาพการให้บริการ ต้นทุน ผลลัพธ์ และอัตราการใช้งาน
	• ยุทธศาสตร์ต้องส่งเสริมมาตรฐานที่จัดทำขึ้น สำหรับรูปแบบการดำเนินงานในอนาคต

มุมมองด้านการดำเนินงาน (Implementation Perspective)	• ยุทธศาสตร์ต้องมีพันธกิจและวิสัยทัศน์ที่ทุกภาคส่วนที่เกี่ยวข้องต้องปฏิบัติตาม โดยต้องมีระยะเวลาการดำเนินงานที่ผ่านการวางแผนมาเป็นอย่างดี และสามารถส่งเสริมแผนงานอื่นๆ ได้ด้วย
	• ยุทธศาสตร์ควรมีการดำเนินงานโดยคำนึงถึงเป้าหมายควบคู่กับประเด็นต่างๆ ของการดำเนินงานและปัญหาที่ต้องเผชิญ
	• ยุทธศาสตร์ต้องให้ความสำคัญกับประเด็นปัญหาและต้องดำเนินแนวทางที่สามารถปฏิบัติได้จริงในการพัฒนาศูนย์ข้อมูล
	• ยุทธศาสตร์ต้องระบุวิธีการให้บริการที่ดีขึ้นตามรูปแบบการดำเนินงานที่มีประสิทธิภาพสูงสุด และระบุวิธีที่จะพัฒนารูปแบบเหล่านี้ให้ดียิ่งขึ้น

12. ความคุ้มค่าและประโยชน์ของโครงการ

โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization หรือ GDCM) จะส่งผลให้เกิดประโยชน์เพื่อเพิ่มประสิทธิภาพขององค์ประกอบต่างๆ เช่น อัตราการใช้ประโยชน์โครงสร้างพื้นฐาน เทคโนโลยี ความปลอดภัยของข้อมูลความมั่นคงระดับประเทศ ความปลอดภัยของข้อมูลและระบบต่างๆ ทางเลือกในการให้บริการ ความพร้อมใช้งาน ความยั่งยืน ความยืดหยุ่นของการบริการ การกู้คืนภัยพิบัติ ความต่อเนื่องการดำเนินงาน และอาคารสถานที่ โดยโครงการนี้จะเพิ่มประสิทธิภาพต้นทุนสำหรับภาครัฐโดยรวมและหน่วยงานในระดับต่างๆ นอกจากนี้ โครงการนี้จะประหยัดงบประมาณการลงทุนโครงสร้างพื้นฐานด้าน IT ต้นทุนการดำเนินงานในด้านทรัพยากรมนุษย์ การซ่อมบำรุง การปฏิบัติงาน การใช้พลังงานและการเพิ่มอัตราการใช้ประโยชน์จากเครือข่าย

โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) จะส่งผลให้เกิดประโยชน์ในด้านต่างๆ ดังต่อไปนี้

การนำมาตรฐานมาใช้ (Adoption of Standards)

การดำเนินงานรูปแบบใหม่จะเอื้อให้การนำมาตรฐานมาใช้ได้อย่างมีประสิทธิภาพมากขึ้น ตามแนวทางที่ได้จัดทำขึ้นสำหรับศูนย์ข้อมูลของหน่วยงาน ถึงแม้ว่า ศูนย์ข้อมูลของหน่วยงานต่างๆ อาจอยู่ในระยะที่ต่างกันในการนำมาตรฐานมาใช้ (Standards Adoption Cycle) หน่วยงานยังสามารถได้รับประโยชน์ตั้งแต่ต้นจากการใช้มาตรฐานเพื่อเพิ่มประสิทธิภาพด้านพลังงาน นอกจากนี้ ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) จะถูกจัดตั้งขึ้นโดยอาศัยมาตรฐานและคุณภาพของโครงสร้างพื้นฐานในระดับที่สูงกว่า ซึ่งนำไปสู่การพัฒนาโครงสร้างพื้นฐานสำหรับอนาคต

การรักษาความปลอดภัยอย่างสูงสุด (No Compromise on Security)

การดำเนินงานรูปแบบใหม่จะส่งเสริมการจัดการรักษาความปลอดภัยข้อมูลภาครัฐ โดยมุ่งเน้นการรักษาความปลอดภัยเป็นหัวใจสำคัญ (Security Centric) นอกจากนี้ จะมีการลงทุนเพื่อจัดทำมาตรฐานความปลอดภัยที่สูงขึ้นสำหรับข้อมูลความมั่นคงระดับประเทศ และจะมีการจัดการข้อมูลที่มีความสำคัญในระดับต่างๆ อย่างเหมาะสมเช่นกัน

การเพิ่มพื้นที่จัดเก็บข้อมูล (Capacity Improvement)

เนื่องจากความต้องการพื้นที่จัดเก็บข้อมูลเพิ่มขึ้นอย่างรวดเร็ว ความสามารถในการรองรับการขยายตัวของบริการ (Scalability) จึงเป็นทิศทางอนาคตของโครงสร้างพื้นฐานและการดำเนินงานของ GDCM นอกจากนี้ พื้นที่จัดเก็บข้อมูลจะถูกยกระดับขึ้นเพื่อรองรับการเติบโตในอนาคต โดยการประยุกต์ใช้มาตรฐาน การใช้งานร่วมกัน การบริการโดยหน่วยงานภายนอก (3rd Party Services) และการบริการโดยภาครัฐ (G-Services)

การใช้ประโยชน์จากโครงสร้างพื้นฐานภาครัฐ (Utilization of Government Infrastructure)

ในปัจจุบัน โครงสร้างพื้นฐานข้อมูลภาครัฐยังขาดการใช้งานอย่างมีประสิทธิภาพ โครงการ GDCM จะเอื้อให้เกิดอัตราการใช้งานโครงสร้างพื้นฐานข้อมูลภาครัฐที่สูงขึ้นจากการใช้บริการร่วมกัน (Shared Services) ซึ่งผลตอบแทนที่สูงขึ้นจากการลงทุนนั้น จะส่งผลให้ภาครัฐสามารถนำงบประมาณไปพัฒนาในทางเลือกอื่นๆ เพื่อประโยชน์โดยรวมของประเทศ

การเพิ่มประสิทธิภาพต้นทุน (Cost Optimization)

ด้วยการดำเนินงานรูปแบบใหม่ หน่วยงานสามารถเพิ่มประสิทธิภาพการใช้งบประมาณโครงสร้างพื้นฐาน โดยอาศัยการบริหารจัดการพื้นที่จัดเก็บข้อมูลอย่างมีประสิทธิภาพ ซึ่งแนวทางดังกล่าวส่งผลให้องค์ประกอบต้นทุนต่างๆ ลดลง เช่น โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ พลังงาน ทรัพยากรบุคคล ฮาร์ดแวร์ และซอฟต์แวร์ เป็นต้น

การมุ่งเน้นภารกิจหลัก (Focus on Core Activities)

การดำเนินงานรูปแบบใหม่จะส่งผลให้หน่วยงานต่างๆ สามารถมุ่งเน้นการปฏิบัติหน้าที่หลักและให้ความสำคัญต่อการบริการประชาชนได้มากขึ้น ดังนั้น ภาระด้านการบริหารจัดการและการซ่อมบำรุงโครงสร้างพื้นฐานด้าน IT ที่ไม่จำเป็นจะถูกยกเลิกไปเพื่อดำเนินภารกิจอื่นที่มีความสำคัญต่อหน่วยงานมากกว่า

การรวมกลุ่มในเชิงสถานที่ตั้ง (Location-based Aggregation)

ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) จะถูกพัฒนาขึ้นและถูกยกระดับโครงสร้างพื้นฐานตามความใกล้เคียงกันในเชิงสถานที่ตั้งและตามประโยชน์ที่จะได้รับจากการจัดการพื้นที่จัดเก็บข้อมูลร่วมกัน (Economies of Scale) ซึ่งการดำเนินงานรูปแบบใหม่ในลักษณะนี้ ภาครัฐสามารถบูรณาการข้อมูลและแอปพลิเคชันที่มีความสำคัญต่อพันธกิจได้อย่างมีประสิทธิภาพ

เป้าหมายของการพัฒนาศูนย์ข้อมูลภาครัฐคือ การยกระดับประสิทธิภาพการปฏิบัติงาน ยกระดับการรักษาความปลอดภัย เพิ่มประสิทธิภาพการใช้จ่ายงบประมาณและต้นทุนการดำเนินงาน นอกจากนี้ เป้าหมายของการพัฒนาศูนย์ข้อมูลภาครัฐยังอาจรวมถึง การเอื้ออำนวยให้โครงสร้างพื้นฐานภาครัฐสามารถรองรับความท้าทายด้านข้อมูล ความต้องการของประชาชน ความซับซ้อนของข้อมูล และต้นทุนที่เพิ่มสูงขึ้นได้อย่างมีประสิทธิภาพ

เป้าหมายหลักของยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐคือ การพัฒนาแนวทางโครงสร้างพื้นฐานด้านข้อมูล เพื่อปกป้องข้อมูลที่ต้องการความปลอดภัยสูงของประเทศและก่อให้เกิดความเป็นเลิศในการบริการ นอกจากนี้ องค์ประกอบอื่นๆ ที่มีความสำคัญเพื่อให้บรรลุเป้าหมายคือ ความยั่งยืนของการดำเนินงานในระยะยาว ประสิทธิภาพด้านต้นทุน นวัตกรรมทางเทคโนโลยี และความพร้อมในการรับมือวิวัฒนาการด้านข้อมูล เป็นต้น

หน่วยงานส่วนใหญ่ดูแลรับผิดชอบศูนย์ข้อมูลมากกว่าหนึ่งแห่งขึ้นไป โดยที่ศูนย์ข้อมูลเหล่านั้นมีระดับประสิทธิภาพที่แตกต่างกัน และบุคลากรของหน่วยงานที่ต้องรับผิดชอบในหลายหน้าที่รวมถึงการดูแลศูนย์ข้อมูลด้วย นอกจากนี้ แต่ละหน่วยงานต้องรับผิดชอบต่อความต้องการด้านข้อมูลที่เพิ่มขึ้นโดยอาศัยโครงสร้างพื้นฐานที่มีอยู่เดิมอย่างจำกัด ในขณะที่หลายประเทศมีเทคโนโลยีที่ทันสมัยและมีโครงสร้างพื้นฐานที่พร้อมต่อการใช้งาน หน่วยงานภาครัฐไทยมีการดำเนินงานโดยขาดการวางแผนด้านการบริหารจัดการข้อมูลและศูนย์ข้อมูลที่มีประสิทธิภาพในระยะยาว ส่งผลให้เกิดภาวะการสิ้นเปลืองของทรัพยากรและการใช้โครงสร้างพื้นฐานที่ขาดประสิทธิภาพอาจก่อให้เกิดปัญหาตามมา เช่น ปัญหาด้านความปลอดภัย ต้นทุนการดำเนินงานที่สูงขึ้น การขาดแคลนบุคลากร และค่าใช้จ่ายพลังงานไฟฟ้าที่สูง นอกจากนี้ ข้อจำกัดในการของบประมาณจากภาครัฐ การรักษาความปลอดภัย การเพิ่มพูนทักษะบุคลากร การจัดการปริมาณข้อมูลที่เพิ่มขึ้น การรองรับความต้องการของผู้ใช้งาน และอัตราการใช้ประโยชน์จากทรัพยากรเทคโนโลยีสารสนเทศ (IT) ที่ต่ำนั้น ล้วนเป็นอุปสรรคต่อการดำเนินงาน ดังนั้น ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (Government Data Center Modernization Strategy) จึงมีความสำคัญเป็นอย่างยิ่ง นอกจากนี้ การจัดเก็บข้อมูลนั้นมีบทบาทสำคัญเพิ่มขึ้นอย่างต่อเนื่อง มีอัตราการเติบโตโดยประมาณที่ 25% ต่อปี ด้วยเหตุนี้ จึงมีความจำเป็นที่ต้องตอบโจทย์สำคัญว่าศูนย์ข้อมูลของหน่วยงานจะสนับสนุนภารกิจหลักของหน่วยงานและภาครัฐได้อย่างไร ดังนั้นยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐต้องนำเสนอแผนที่มีความครอบคลุม ความบูรณาการ และความยั่งยืน เพื่อเอื้ออำนวยให้โครงสร้างพื้นฐานด้านข้อมูลภาครัฐมีประสิทธิภาพสูงสุดในการทำงาน

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐตอบโจทย์สำคัญ ข้อกังวล ความต้องการ และข้อจำกัดต่างๆ ที่หน่วยงานภาครัฐกำลังเผชิญอยู่ทุกวันนี้ได้ ยุทธศาสตร์นี้ไม่เพียงแต่ครอบคลุมการให้บริการผ่านแนวทางและวิธีการทางเลือก แต่ยังเอื้อให้เกิดการใช้มาตรฐานทางเทคโนโลยีเพื่อสร้างระบบที่มีความคล่องตัว การตอบสนองรวดเร็ว การบูรณาการ ความยั่งยืน ความปลอดภัย การบริหารจัดการ และความพร้อมการรองรับอนาคต

แผนยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐสำหรับประเทศไทยถูกจัดทำขึ้นบนพื้นฐานความเข้าใจอย่างลึกซึ้งในโครงสร้างพื้นฐานด้านข้อมูลภาครัฐที่มีอยู่ในปัจจุบัน อันประกอบด้วย ศูนย์ข้อมูลประจำหน่วยงาน การใช้บริการคลาวด์ของหน่วยงานภายนอก การใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก และการใช้บริการ G-Cloud ที่หน่วยงานต่างๆ ใช้งานอยู่ในปัจจุบัน ซึ่งบริการเหล่านี้รองรับความต้องการข้อมูลทั้งหมดสำหรับภาครัฐและการให้บริการแก่ประชาชน แต่อย่างไรก็ตาม การขยายตัวของข้อมูล ความซับซ้อนที่เพิ่มขึ้น ความต้องการการบริการ และข้อจำกัดในการดำเนินงานของหน่วยงานต่างๆ เป็นประเด็นสำคัญที่ต้องแก้ไขโดยการจัดตั้งโครงสร้างพื้นฐานที่ยกระดับศักยภาพของภาครัฐให้สอดคล้องกับแนวทางพัฒนาเศรษฐกิจดิจิทัล

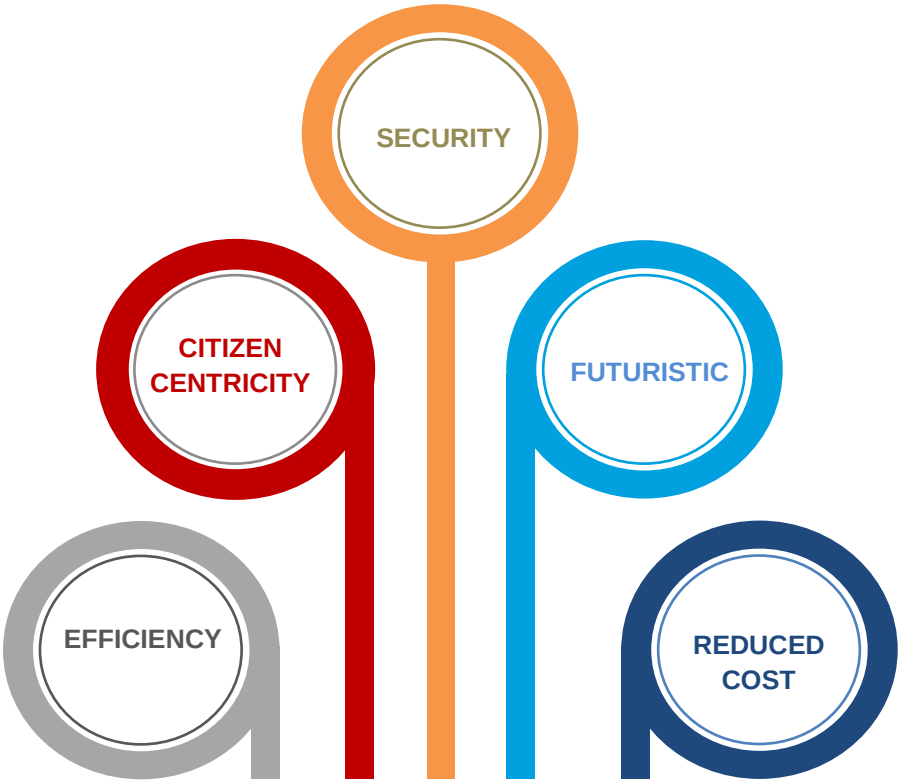
ความต้องการและข้อจำกัดของหน่วยงานภาครัฐ

รัฐบาลในหลายประเทศทั่วโลกเล็งเห็นความจำเป็นที่ต้องเปิดรับเทคโนโลยีและนวัตกรรมใหม่ รวมถึงการใช้บริการต่างๆ ร่วมกัน เพื่อขับเคลื่อนการพัฒนาเศรษฐกิจดิจิทัลและส่งเสริมการใช้ชีวิตที่ยั่งยืนสำหรับประชาชน

โครงการพัฒนาศูนย์ข้อมูลภาครัฐก่อให้เกิดโครงสร้างพื้นฐานทันสมัย เนื่องจากการกำหนดมาตรฐานและการประยุกต์ใช้ รวมถึงการใช้ประโยชน์จากโครงสร้างพื้นฐานด้านข้อมูลในอนาคต 6 รูปแบบดังต่อไปนี้ ให้เกิดประสิทธิภาพ

(1) ศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center)
(2) ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center)
(3) ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center)
(4) การบริการพื้นที่วางเครื่องแม่ข่าย/จัดเก็บข้อมูลโดยหน่วยงานภายนอก (3rd Party Colocation/Physical Hosting)
(5) การบริการโดยหน่วยงานภายนอก (3rd Party Services)
(6) การบริการโดยภาครัฐ (G-Services)

หากมีการใช้องค์ประกอบเหล่านี้ทั้งหมดรวมกันอย่างมีประสิทธิภาพ จะส่งผลให้เกิดประโยชน์แก่ภาครัฐดังต่อไปนี้



ประสิทธิภาพ (EFFICIENCY)

ประสิทธิภาพ (EFFICIENCY) เกิดจากการใช้พื้นที่จัดเก็บข้อมูลอย่างมีประสิทธิภาพ (Economies of Scale) โครงสร้างพื้นฐานที่มีความคล่องตัว (Agile Infrastructure) การดำเนินงานที่มีความยืดหยุ่นและมีความสะดวกการให้บริการที่มีประสิทธิภาพ การใช้ทรัพยากรอย่างคุ้มค่า โครงสร้างพื้นฐานที่มีประสิทธิภาพสูงขึ้น และการมีอัตราการใช้งานสูงขึ้น

ประชาชนเป็นศูนย์กลาง (CITIZEN CENTRICITY)

ประชาชนเป็นศูนย์กลาง (CITIZEN CENTRICITY) เกิดจากการให้บริการแบบครบวงจร การยกระดับความพร้อมใช้งาน การเตรียมการสำหรับบริการใหม่ที่มีประสิทธิภาพสูงขึ้น การยกระดับประสบการณ์ของผู้ใช้งาน (User Experience) ผ่านการเข้าถึงข้อมูลที่สะดวกและการมีข้อมูลที่น่าเชื่อถือ

ความปลอดภัย (SECURITY)

ความปลอดภัย (SECURITY) เกิดจากการส่งเสริมการปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยข้อมูลภาครัฐ และการพัฒนาความสามารถในการรองรับนโยบายด้านการรักษาความมั่นคงปลอดภัยใหม่ๆ

การรองรับอนาคต (FUTURISTIC)

การรองรับอนาคต (FUTURISTIC) เกิดจากโครงสร้างพื้นฐานด้านข้อมูลที่มีความยืดหยุ่นและคล่องตัว โดยอาศัยเทคโนโลยีใหม่ที่ยั่งยืน สามารถพัฒนาและเพิ่มประสิทธิภาพได้อย่างทันท่วงที

การเพิ่มประสิทธิภาพต้นทุน (OPTIMIZED COST)

การเพิ่มประสิทธิภาพต้นทุน (OPTIMIZED COST) เกิดจากการใช้งานโครงสร้างพื้นฐานในอัตราที่สูงขึ้นและการใช้ประโยชน์จากรูปแบบโครงสร้างพื้นฐานด้านข้อมูลทางเลือก ที่สามารถเพิ่มประสิทธิภาพในการใช้จ่ายด้านการลงทุนและการดำเนินงานในอนาคตได้

13. แผนพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

แผนพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) สำหรับประเทศไทย จะเสนอยุทธศาสตร์การบริการศูนย์ข้อมูลและการนำมาตรฐานมาประยุกต์ใช้โดยผ่านการวางแผนอย่างรอบคอบ ซึ่งแผนพัฒนาดังกล่าวมีผลกระทบต่อกระทรวงและหน่วยงานต่างๆ โดยอาจมีแนวโน้ม ข้อจำกัด และประเด็นที่กระทบหน่วยงานแตกต่างกันในแต่ละหน่วยงาน นอกจากนี้ แผนพัฒนาศูนย์ข้อมูลภาครัฐจะขับเคลื่อนการเปลี่ยนแปลง และกำหนดสมมติฐานสำหรับยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐในภาพรวม

การให้บริการในอนาคตนั้นเกี่ยวข้องกับวิธีการบริหารจัดการและสถานที่จัดเก็บข้อมูลที่มีอยู่ โดยมุ่งเน้นความมั่นคงปลอดภัย ดังนั้น การดำเนินงานในอนาคตจำเป็นต้องจำแนกประเภทข้อมูลและกำหนดกรอบสำหรับแต่ละหน่วยงานอย่างชัดเจน ยุทธศาสตร์นี้มุ่งตอบโจทย์ใน 2 มิติที่สำคัญคือ 1) ประเภทของการให้บริการ และ 2) กลไกการให้บริการ ซึ่งครอบคลุมการเพิ่มประสิทธิภาพต้นทุนและการยกระดับการให้บริการ นอกจากนี้ หน่วยงานภาครัฐไทยมีศูนย์ข้อมูลเป็นของตนเองจำนวนมาก ซึ่งศูนย์ข้อมูลเหล่านี้สามารถนำมาใช้ประโยชน์ให้เกิดประสิทธิภาพสูงสุดได้

หนึ่งในเป้าหมายสำคัญของแผนพัฒนาศูนย์ข้อมูลภาครัฐคือ การเพิ่มประสิทธิภาพการใช้งานศูนย์ข้อมูลที่มีอยู่เดิมซึ่งอาจมีข้อจำกัดในแง่ขนาดของศูนย์ข้อมูลและพื้นที่จัดเก็บข้อมูล ดังนั้น เมื่อพิจารณาจากประเภทและระดับความปลอดภัยของข้อมูล โครงสร้างพื้นฐานศูนย์ข้อมูลปัจจุบันต้องถูกกำหนดกรอบการใช้งาน การบริหารจัดการพื้นที่จัดเก็บข้อมูล การลงทุนในอนาคต และเจตนารมณ์เชิงยุทธศาสตร์

ด้วยเหตุนี้ แผนพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) จึงเสนอทิศทางอนาคตให้มีการพัฒนา 6 รูปแบบการดำเนินงานในอนาคตของโครงสร้างพื้นฐานด้านข้อมูลซึ่งประกอบกันทั้งหมดเป็น **ระบบศูนย์ข้อมูลภาครัฐไทย (Thailand Government Data Center Ecosystem)** ระบบใหม่นี้ประกอบด้วยรูปแบบการดำเนินงานต่างๆ ที่หน่วยงานสามารถเลือกใช้จัดเก็บข้อมูลปัจจุบันและอนาคตได้ ทั้งนี้ ในมุมมองของการให้บริการ บทบาทของหน่วยงาน และบทบาทของภาครัฐนั้น จะมีการอธิบายเนื้อหาในส่วนต่อไป ซึ่งสามารถใช้เป็นแนวทางการให้บริการได้อย่างมีประสิทธิภาพ

การใช้งานศูนย์ข้อมูลระดับหน่วยงาน

ปัจจุบัน ศูนย์ข้อมูลภาครัฐของไทยมีการใช้งานบนโครงสร้างพื้นฐานหลากหลายรูปแบบ ได้แก่ 1) ศูนย์ข้อมูลประจำหน่วยงาน (Agecny Own Data Center) 2) การใช้บริการคลาวด์ภาครัฐ (G-Cloud) 3) การใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) และ 4) การใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) โดยจาก 42 หน่วยงานที่เข้าร่วมการประชุมระดมความคิดเห็นกลุ่มย่อยโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) นั้น 90% ของหน่วยงานระบุว่าหน่วยงานมีการใช้ศูนย์ข้อมูลประจำหน่วยงาน (Agecny Own Data Center) ในการจัดเก็บและประมวลผลข้อมูลของหน่วยงาน ขณะที่อีก 20% ของหน่วยงานระบุว่าหน่วยงานของตนใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) และใช้บริการคลาวด์ภาครัฐ (G-Cloud) ในสัดส่วนที่เท่ากัน และมีเพียง 7% ที่ใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud)

ทิศทางการดำเนินงานโครงสร้างพื้นฐานภาครัฐของไทยในอนาคตจะมุ่งเน้นการเพิ่มอัตราการใช้ประโยชน์จากทรัพยากรที่มีอยู่เดิมภายในหน่วยงาน ซึ่งปัจจุบันยังไม่ได้ถูกนำมาใช้งานอย่างเต็มประสิทธิภาพ ปัญหาสำคัญที่อาจเป็น

อุปสรรคในการใช้งานศูนย์ข้อมูลเดิมได้อย่างมีประสิทธิภาพคือ การขาดมาตรฐานบริการศูนย์ข้อมูลอันเป็นที่ยอมรับร่วมกัน ความซับซ้อนในการเชื่อมโยงเครือข่าย ประเด็นการจำแนกประเภทข้อมูล ความท้าทายในการจัดการความปลอดภัยข้อมูล และการขาดความสามารถในการประเมินและวางแผนอัตราการใช้งานในอนาคต นอกจากนี้หน่วยงานมีการใช้เทคโนโลยี Virtualization สำหรับการให้บริการของตนเอง ด้วยเหตุนี้การทำ Virtualization จึงนับเป็นโอกาสในการจัดทำแพลตฟอร์มร่วมกันในรูปแบบของศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) ซึ่งศูนย์ข้อมูลในลักษณะนี้จะส่งเสริมให้การย้ายการให้บริการสามารถทำได้ง่ายขึ้น เพื่อรองรับการขยายการให้บริการสู่ระดับกระทรวงหรือข้ามหน่วยงาน แนวทางนี้จะเป็นกุญแจสำคัญที่เพิ่มประสิทธิภาพการใช้ทรัพยากร โดยแพลตฟอร์มดังกล่าวจำเป็นต้องมีมาตรฐานร่วมกันและสามารถทำงานร่วมกันได้ (Interoperability) นอกจากนี้ การจัดซื้อระบบ Virtualization ในระดับประเทศอาจมีประโยชน์มากกว่า เมื่อเทียบกับการจัดซื้อในระดับหน่วยงานของตนเอง

แนวทางเชิงยุทธศาสตร์ที่สำคัญต่อหน่วยงานและภาครัฐ มีดังนี้

- ศูนย์ข้อมูลประจำหน่วยงานจะต้องปฏิบัติตามแนวทางการให้บริการ การจำแนกประเภทข้อมูล การดูแลรักษา การกำหนดมาตรฐาน การจัดการทรัพยากรบุคคล และการดำเนินงานอย่างมีประสิทธิภาพ โดยเคร่งครัด
- ศูนย์ข้อมูลประจำหน่วยงานบางแห่งจะถูกพัฒนาเป็นศูนย์ข้อมูลระดับกระทรวงหรือศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน ให้สอดคล้องกับหลักเกณฑ์ที่ภาครัฐกำหนดไว้ ซึ่งเป็นส่วนหนึ่งของโครงการ “iTransform”
- หน่วยงานที่ไม่สามารถปฏิบัติตามแนวทางและหลักเกณฑ์ที่กำหนด ควรพิจารณาแนวทางการย้ายข้อมูลไปจัดเก็บไว้ยังศูนย์ข้อมูลในรูปแบบอื่นแทน แล้วทำการยกเลิกหรือปิดบริการศูนย์ข้อมูลของหน่วยงานนั้น
- หน่วยงานจะต้องปฏิบัติตามแผนการเปลี่ยนแปลงตามแผนยุทธศาสตร์อย่างเคร่งครัด
- หน่วยงานจะต้องดำเนินการศึกษาเชิงสำรวจในปีที่ 1 เพื่อระบุความต้องการในการจำแนกประเภทข้อมูล จัดเตรียมแผนการดำเนินงานสำหรับศูนย์ข้อมูลของหน่วยงาน และดำเนินการศึกษาความเป็นไปได้ในการย้ายข้อมูลตามข้อกำหนดและประเภทของแอปพลิเคชัน ไปยังรูปแบบทางเลือกอื่น โครงการนี้จะใช้ชื่อว่า “iDiscover”
- หน่วยงานจะต้องดำเนินการศึกษาความเป็นไปได้ในการประยุกต์ใช้มาตรฐานตามขั้นตอนของการนำมาตรฐานมาใช้ เมื่อวางแผนเสร็จสิ้น หน่วยงานจะต้องปฏิบัติให้สอดคล้องกับแนวทางและหลักเกณฑ์ที่กำหนด โครงการนี้จะใช้ชื่อว่า “iAdopt”
- หน่วยงานจะต้องระบุความต้องการทรัพยากรบุคคลและทรัพยากรอื่นที่สามารถใช้ร่วมกับโครงสร้างพื้นฐานรูปแบบอื่น การศึกษานี้จะเป็นส่วนหนึ่งของโครงการ “iTransition”
- หน่วยงานจะต้องใช้งานศูนย์ข้อมูลประจำหน่วยงานในการจัดเก็บข้อมูลให้เหมาะสมกับประเภทข้อมูล
- หน่วยงานต้องระบุแนวทางในการย้ายข้อมูลทั่วไป เพื่อจัดเก็บไว้ที่การบริการโดยภาครัฐ (G-Services) หรือ ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) หรือ ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) หรือ การบริการโดยหน่วยงานภายนอก (3rd Party Services) โดยเป็นการดำเนินงานส่วนหนึ่งในโครงการ “iOptimize”

การพัฒนาศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน

ปัจจุบันศูนย์ข้อมูลของหน่วยงานภาครัฐไทยเผชิญประเด็นสำคัญด้านอัตราการใช้งาน ด้านพื้นที่จัดเก็บข้อมูลเกินความจำเป็น และด้านการเตรียมความพร้อมรองรับการขยายตัวของบริการ ในบางกรณีหน่วยงานที่มีศูนย์ข้อมูลแห่งเดียวอาจมีอัตราการใช้งานเครื่องแม่ข่ายเฉลี่ยที่ต่ำกว่า 5% ดังนั้นการพัฒนาศูนย์ข้อมูลจึงเป็นโอกาสให้เกิดการใช้ทรัพยากรที่มีอยู่เดิมให้เกิดประสิทธิภาพมากขึ้น และเป็นโอกาสที่จะบริหารการจัดซื้ออุปกรณ์ IT ใหม่ในอนาคตได้อย่างเหมาะสม

การพัฒนาบริการร่วมกันสำหรับภาครัฐไทยนั้นมีต้นกำเนิดจากศูนย์ข้อมูลขนาดใหญ่ ที่มีความจำเป็นต้องชี้แจงในการของบประมาณและการใช้จ่าย และรวมถึงการต้องเป็นตัวอย่างที่ดีในการเปิดโครงสร้างพื้นฐานและทรัพยากรให้แก่หน่วยงานใช้งานร่วมกัน

โครงสร้างพื้นฐานที่ใช้งานร่วมกันในรูปแบบศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) จะมีพื้นที่ขนาดใหญ่ (500 ตร.ม. ขึ้นไป) และปฏิบัติตามแนวทางมาตรฐานที่ระบุในภาคผนวก

การให้การบริการร่วมกันจะส่งผลให้เกิดประโยชน์หลายประการ ดังนี้

- ✓ *ขับเคลื่อนการปฏิบัติตามมาตรฐานซึ่งเป็นที่ยอมรับ*
- ✓ *สามารถตอบสนองความต้องการศูนย์ข้อมูลได้อย่างรวดเร็ว (On-demand Ready)*
- ✓ *มีความพร้อมใช้งานสูง เพื่อสามารถดำเนินงานตลอดเวลา 24 ชั่วโมง 7 วันต่อสัปดาห์*
- ✓ *การเชื่อมต่อเครือข่ายความเร็วสูงไปยังเครือข่ายภาครัฐ*
- ✓ *ความปลอดภัยทางกายภาพและการสำรองข้อมูล เพื่อให้ดำเนินงานได้อย่างราบรื่น*
- ✓ *มีการรายงานการให้บริการเปรียบเทียบกับข้อตกลงระดับการให้บริการที่กำหนดไว้ (Service Level Agreement)*
- ✓ *ต้นทุนทั้งหมด (Total Cost of Ownership) ลดลง*
- ✓ *เพิ่มประสิทธิภาพการใช้ทรัพยากร (ทรัพยากรบุคคลและทรัพยากรด้านเทคโนโลยี เช่น ฮาร์ดแวร์และซอฟต์แวร์)*
- ✓ *สามารถรองรับปริมาณข้อมูลและการประมวลผลที่สูง*
- ✓ *อัตราการใช้ทรัพยากรที่มีประสิทธิภาพ*

แนวทางเชิงยุทธศาสตร์ที่สำคัญต่อหน่วยงานและภาครัฐ มีดังนี้

- ❖ ตัวแทนภาครัฐดำเนินการศึกษาความเป็นไปได้ วิเคราะห์ และระบุศูนย์ข้อมูลที่พร้อมพัฒนาไปสู่ศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) หรือศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) ภายใต้โครงการ “iDiscover”
- ❖ หน่วยงานต้องปฏิบัติตามคำสั่งภาครัฐในการพัฒนาศูนย์ข้อมูลของหน่วยงานไปสู่ศูนย์ข้อมูลระดับกระทรวงหรือศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน
- ❖ หน่วยงานต้องสามารถใช้งานศูนย์ข้อมูลที่ให้บริการร่วมกัน (ศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน) เพื่อจัดเก็บข้อมูลตามประเภทที่เหมาะสม

- หน่วยงานต้องจัดเตรียมทรัพยากร โครงสร้างพื้นฐาน และบุคลากร เพื่อร่วมเป็นส่วนหนึ่งของการดำเนินงานด้านโครงสร้างพื้นฐาน
- เจ้าหน้าที่กำกับดูแลการดำเนินงาน (Governance Committee) สำหรับศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงานต้องขับเคลื่อนการให้บริการร่วมกันตามแนวทางและมาตรฐานที่กำหนดในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards)
- เจ้าหน้าที่กำกับดูแลการดำเนินงานต้องกำหนดเกณฑ์และกลไกการกำกับดูแล เพื่อประเมินประสิทธิภาพการทำงานของศูนย์ข้อมูลที่เทียบเท่า SLA ที่กำหนดไว้
- เจ้าหน้าที่กำกับดูแลการดำเนินงานต้องทำให้มั่นใจว่าศูนย์ข้อมูลถูกพัฒนาเป็นศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน ภายในกรอบเวลาที่กำหนดไว้ในแผนการดำเนินงานภายใต้โครงการ “iAdopt”
- หน่วยงานภายใต้กระทรวงเดียวกันที่มีศูนย์ข้อมูลระดับกระทรวงจำเป็นต้องใช้งานศูนย์ข้อมูลดังกล่าวอย่างมีประสิทธิภาพและจัดเก็บข้อมูลของหน่วยงานที่ไม่น้อยกว่า 10% ไว้กับศูนย์ข้อมูลระดับกระทรวง
- เจ้าหน้าที่กำกับดูแลการดำเนินงานต้องกำหนด “ขอบเขต” ความครอบคลุมของศูนย์ข้อมูลให้บริการระหว่างหน่วยงานและหน่วยงานใดๆ (หน่วยงานอิสระหรือกระทรวง) ที่จะอยู่ภายใต้ขอบเขตการดำเนินงานของศูนย์ข้อมูลลักษณะนี้
- หน่วยงานที่อยู่ภายใต้ขอบเขตของศูนย์ข้อมูลให้บริการระหว่างหน่วยงานจะต้องจัดเก็บข้อมูลของหน่วยงานที่ไม่น้อยกว่า 10% ไว้กับศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน โดยเป็นการดำเนินงานส่วนหนึ่งภายใต้โครงการ “iOptimize”
- เจ้าหน้าที่กำกับดูแลการดำเนินงานต้องผลักดันให้เกิดการจัดตั้งศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน มีการดำเนินงาน มีการให้บริการ และมีการใช้งานตามระยะเวลาที่ระบุไว้ในแผนการดำเนินงาน

การลดปริมาณการใช้บริการพื้นที่วางเครื่องแม่ข่าย (Colocation)

หน่วยงานภาครัฐหลายแห่งใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) ผลสะท้อนจากความคิดเห็นในการสำรวจพบว่า 20% ของหน่วยงานใช้การบริการดังกล่าวในการจัดเก็บข้อมูลบางส่วน สำหรับ Colocation นั้น หน่วยงานขนาดเล็ก (มีปริมาณข้อมูลไม่มาก) จะได้รับประโยชน์จากความก้าวหน้าทางเทคโนโลยีในระดับเดียวกับหน่วยงานขนาดใหญ่ โดยไม่มีภาระเพิ่มเติมในการจัดเก็บและดูแลรักษาอุปกรณ์ภายใน อย่างไรก็ตาม หน่วยงานส่วนใหญ่ที่ใช้บริการ Colocation มักมีการดำเนินการศูนย์ข้อมูลประจำหน่วยงาน (Agency Own Data Center) เช่นกัน

การใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) ส่งผลให้เกิดประโยชน์หลายประการดังนี้

- ✓ *หน่วยงานมุ่งเน้นการดำเนินงานตามภารกิจได้มากขึ้น*
- ✓ *จัดจ้างผู้ให้บริการภายนอก เพื่อตอบสนองความต้องการด้านบุคลากรของหน่วยงานสำหรับการดูแลรักษาข้อมูล*
- ✓ *โครงสร้างพื้นฐานที่มีการบริหารจัดการอย่างมีประสิทธิภาพและมีเสถียรภาพช่วยลดความต้องการและการพึ่งพาความช่วยเหลือด้าน IT แบบ Onsite รวมถึงยังมีการใช้ระบบสื่อสารข้อมูลและทรัพยากรร่วมกัน*

- ✓ *เป็นทางเลือกในการขยายพื้นที่จัดเก็บข้อมูล เพื่อเพิ่มทรัพยากร*
- ✓ *ลดความเสี่ยง*
- ✓ *ประหยัดต้นทุน*

ในบริบทของประเทศไทย การใช้บริการพื้นที่วางเครื่องแม่ข่าย (Colocation) เป็นที่นิยมแพร่หลาย แม้มีการลงทุนในการสร้างโครงสร้างพื้นฐานศูนย์ข้อมูลอยู่แล้วก็ตาม ดังนั้น จากรูปแบบการจัดเก็บข้อมูลที่หลากหลาย เช่น ศูนย์ข้อมูลประจำหน่วยงานที่ได้มาตรฐานและมีความปลอดภัย ศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงานซึ่งให้การบริการอย่างมีประสิทธิภาพ การบริการโดยหน่วยงานภายนอก (3rd Party Services) และการบริการโดยภาครัฐ (G-Services) ที่ครอบคลุม Colocation นั้น หน่วยงานต่างๆ จึงมีหลายทางเลือกที่จะใช้บริการจัดเก็บข้อมูลที่เทียบเท่าหรือดีกว่า Colocation

ดังนั้น ในเชิงยุทธศาสตร์ เมื่อพิจารณาต้นทุนการดำเนินงานและความพร้อมใช้งานของทางเลือกอื่นๆ ที่มีความเหมาะสมแล้วนั้น จึงแนะนำให้ลดการใช้บริการพื้นที่วางเครื่องแม่ข่ายของหน่วยงานภายนอก (3rd Party Colocation) ลง ซึ่งเป็นการดำเนินงานส่วนหนึ่งภายใต้แผนยุทธศาสตร์ GDCM

แนวทางเชิงยุทธศาสตร์ที่สำคัญต่อหน่วยงานและภาครัฐ มีดังนี้

- ❖ หน่วยงานต่างๆ ต้องลดการพึ่งพาและการจัดเก็บข้อมูลไว้กับ 3rd Party Colocation
- ❖ จะไม่มีการอนุญาตหน่วยงานใหม่ให้ใช้บริการ 3rd Party Colocation หากมีความจำเป็นหน่วยงานสามารถใช้บริการ Colocation ของภาครัฐ ซึ่งเป็นส่วนหนึ่งของ G-Services
- ❖ หากหน่วยงานที่ไม่มีศูนย์ข้อมูลของตนเอง แต่มีความต้องการที่จะใช้บริการ 3rd Party Colocation หน่วยงานดังกล่าวจะต้องจัดทำแผนการดำเนินงาน รวมถึงชี้แจงเหตุผลและความจำเป็น
- ❖ หน่วยงานที่ใช้บริการ 3rd Party Colocation อยู่เดิมจะไม่สามารถต่อสัญญาใหม่ เว้นแต่มีความต้องการเฉพาะเจาะจง โดยหน่วยงานจะต้องจัดทำแผนการดำเนินงาน รวมถึงชี้แจงเหตุผลและความจำเป็น
- ❖ แต่ละหน่วยงานที่จัดเก็บข้อมูลไว้กับ 3rd Party Colocation จะต้องจัดเตรียมแผนการย้ายข้อมูลและแผนบรรเทาความเสี่ยง เพื่อลดผลกระทบในการดำเนินงานและการให้บริการ
- ❖ ภาครัฐต้องจัดเตรียมการให้บริการ Colocation เป็นส่วนหนึ่งของการบริการโดยภาครัฐ (G-Services) โดยปฏิบัติตาม SLA มาตรฐานที่ระบุไว้ในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ
- ❖ ภาครัฐต้องจัดเตรียมบริการศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน โดยปฏิบัติตามมาตรฐานที่ระบุไว้ในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ ภายใต้โครงการ “iAdopt”
- ❖ ภาครัฐต้องจัดเตรียมบริการคลาวด์ซึ่งเป็นส่วนหนึ่งของการบริการโดยภาครัฐ (G-Services) โดยปฏิบัติตามมาตรฐานที่ระบุไว้ในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards)
- ❖ หน่วยงานต้องใช้ประโยชน์จากการจัดเก็บข้อมูลรูปแบบอื่นๆ เพื่อความสะดวกในการย้ายข้อมูลและเพิ่มประสิทธิภาพในการนำข้อมูลไปประมวลผลต่อไป ภายใต้โครงการ “iOptimize”

ระบบคลาวด์มีบทบาทสำคัญมากขึ้น

ปัจจุบันภาครัฐในหลายประเทศทั่วโลกเริ่มมีการใช้บริการคลาวด์มากขึ้น เพื่อใช้ประโยชน์จากพื้นที่จัดเก็บข้อมูลและต้นทุนอย่างคุ้มค่า ถึงแม้บริการคลาวด์กำลังเติบโตแบบทวีคูณ แต่หน่วยงานภาครัฐยังคงลังเลที่จะใช้บริการดังกล่าวในการจัดการและจัดเก็บข้อมูล โดยมีประเด็นหลักในเรื่องของการรักษาความปลอดภัยข้อมูลและค่าใช้จ่าย ขณะเดียวกัน รัฐบาลในหลายประเทศได้ลงทุนเม็ดเงินมหาศาลเพื่อสร้างระบบคลาวด์ของตนเอง ในความเป็นจริงเทคโนโลยีคลาวด์กำลังพลิกโฉมการดำเนินงานของหน่วยงานภาครัฐและเปลี่ยนแปลงไปสู่การให้บริการจัดเก็บข้อมูลผ่านทางอินเทอร์เน็ตด้วยการใช้งบประมาณอย่างมีประสิทธิภาพและนวัตกรรมที่ก้าวหน้ามาโดยตลอด จากข้อจำกัดทางด้านงบประมาณในช่วงหลายปีที่ผ่านมา หน่วยงานต่างๆ ทั่วโลกจึงจำเป็นต้องหารูปแบบการดำเนินงานที่มีประสิทธิภาพสูงสุดที่หน่วยงานสามารถการดำเนินงานได้อย่างมีประสิทธิภาพและให้การบริการที่ดีไปพร้อมๆ กันได้ การใช้งานระบบคลาวด์อาจถูกมองว่าแค่สามารถทำให้หน่วยงานควบคุมต้นทุนได้จากการใช้บริการและโครงสร้างพื้นฐานร่วมกันเท่านั้น แต่ในความเป็นจริงหน่วยงานยังสามารถพัฒนาการดำเนินงานต่างๆ เพิ่มเติมเพื่อให้มีการใช้ระบบคลาวด์ได้อย่างมีประสิทธิภาพ ปัจจุบันนอกจากหน่วยงานภาครัฐมีการใช้ระบบคลาวด์ที่เรียกว่า Public Cloud ซึ่งมีลักษณะการให้บริการแบบสาธารณะแล้ว หน่วยงานภาครัฐยังมีการใช้ระบบคลาวด์ที่เรียกว่า Private Cloud ซึ่งมีฟังก์ชันการทำงานคล้ายกับ Public Cloud แต่สามารถรองรับภาระงานที่สำคัญต่อพันธกิจ (Mission Critical Workload) ได้อย่างมีประสิทธิภาพมากกว่า

สำหรับประเทศไทยนั้น หลายหน่วยงานจำเป็นต้องรองรับการดำเนินงานที่สำคัญต่อพันธกิจด้วยการใช้ระบบคลาวด์ที่สามารถรองรับการขยายตัวของการบริการ เทคโนโลยีไร้สาย และเทคโนโลยีการวิเคราะห์ (Analytics) อย่างไรก็ตาม หน่วยงานภาครัฐยังต้องปฏิบัติตามมาตรการความปลอดภัยอย่างเคร่งครัดเพื่อลดความเสี่ยงจากการถูกโจมตีจากทั้งภายในและภายนอก

จากการสำรวจ มีหน่วยงานภาครัฐไทยเพียง 10% ที่ใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) จากผู้ให้บริการ และมีข้อมูลภาครัฐเพียง 2.6% ที่ถูกจัดเก็บไว้บนบริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) จากการประมาณการในปัจจุบัน

อาจถือเป็นเรื่องน่าประหลาดใจจากตัวเลขที่กล่าวมาข้างต้น หากพิจารณาจากประโยชน์หลายประการที่จะได้รับจากระบบคลาวด์ซึ่งสามารถช่วยยกระดับประสิทธิภาพการจัดการข้อมูล ลดต้นทุน และเพิ่มการรักษาความปลอดภัยข้อมูลของหน่วยงานภาครัฐได้

- ✓ *ทรัพยากรที่มีความยืดหยุ่นสนับสนุนการสร้างระบบการดำเนินงานรูปแบบใหม่สำหรับทั้งการใช้งานภายในและภายนอก*
- ✓ *เพิ่มความปลอดภัยและการจัดการข้อมูลอย่างปลอดภัย เนื่องจากการจัดเก็บข้อมูลในระบบคลาวด์ระดับองค์กรรองรับเทคโนโลยีด้านความปลอดภัย เช่น การทำ Data Encryption เป็นต้น*
- ✓ *การรวบรวมข้อมูลสำหรับจัดเก็บไว้บนระบบคลาวด์ถือเป็นโอกาสในการจำแนกประเภทข้อมูลให้ดีขึ้น ทำให้มีการจัดเก็บอย่างมีประสิทธิภาพและสามารถนำข้อมูลไปใช้ประโยชน์ได้อย่างรวดเร็ว*
- ✓ *ลดต้นทุนลงอย่างมีนัยสำคัญ เนื่องจากค่าใช้จ่ายในการดำเนินงานต่ำกว่าการดูแลรักษาศูนย์ข้อมูลเอง*

- ✓ *ใช้เทคโนโลยีที่ทันสมัย*
- ✓ *บุคลากรมีการจัดสรรใช้งานอย่างมีประสิทธิภาพมากขึ้นและสามารถมุ่งเน้นการดำเนินภาระกิจหลัก*

แนวทางเชิงยุทธศาสตร์ที่สำคัญต่อหน่วยงานและภาครัฐ มีดังนี้

- หน่วยงานต่างๆ ต้องเพิ่มสัดส่วนการจัดเก็บข้อมูลทั่วไปไว้บนการบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS)
- หน่วยงานต้องดำเนินการศึกษาความเป็นไปได้ในการจัดเก็บข้อมูลหรือแอปพลิเคชันใหม่ รวมถึงทำการจัดเก็บข้อมูลไว้บนระบบคลาวด์ โดยจะต้องส่งรายงานการศึกษาความเป็นไปได้และผลการดำเนินงานตามแผนที่กำหนดไว้ภายใต้โครงการ iDiscover
- ภาครัฐต้องจัดทำรายชื่อผู้ให้การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) ซึ่งปฏิบัติตาม SLA และมาตรฐาน ในอัตราค่าใช้บริการ (ต้นทุน) ที่มีการเจรจาต่อรองกันเรียบร้อยแล้วและสามารถรองรับการบริการต่างๆ ที่หน่วยงานต้องการได้
- หน่วยงานจะต้องเลือกผู้ให้การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) จากรายชื่อข้างต้นสำหรับจัดเก็บข้อมูล
- หน่วยงานอาจได้รับอนุญาตให้ใช้ผู้ให้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) รายเดิมและการบริการรูปแบบเดิม ในกรณีที่มีความต้องการที่มีความเฉพาะสำหรับหน่วยงานตนเอง
- หน่วยงานต้องจัดเก็บข้อมูลทั่วไปชุดใหม่ไว้ก่อนและย้ายข้อมูลทั่วไปที่มีความเหมาะสมไปจัดเก็บไว้บนการบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS, และ SaaS) อันเป็นผลจากการศึกษาความเป็นไปได้ ภายใต้โครงการ “iOptimize”

การบริการภาครัฐเป็นกรอบแนวคิดใหม่

ภาครัฐได้ให้นิยามการดำเนินงานของตนขึ้นใหม่ในการยกระดับการให้บริการแก่ประชาชน โดยหน่วยงานภาครัฐในหลายประเทศทั่วโลกกำลังเปลี่ยนไปใช้ระบบคลาวด์ที่มีความปลอดภัย มีประโยชน์ต่อการดำเนินงานและการลงทุนอย่างเป็นรูปธรรม ดังนั้น การบริการโดยภาครัฐ (Government Services) ที่ให้การบริการรัฐบาลอิเล็กทรอนิกส์ (e-Government Services) ในรูปแบบต่างๆ คือ โครงสร้างพื้นฐานอิเล็กทรอนิกส์ภาครัฐ (e-Government Infrastructure) ที่หน่วยงานภาครัฐสามารถใช้งานร่วมกัน โดยมีความคล่องตัวและเป็นการใช้งบประมาณอย่างมีประสิทธิภาพ

ภาครัฐไทยได้นำรูปแบบการบริการโดยภาครัฐ (Government Services หรือ G-Services) เพื่อใช้รองรับความต้องการจากภาคประชาชนและภาครัฐที่มีต่อการบริการรัฐบาลอิเล็กทรอนิกส์ (e-Government Services) ที่เพิ่มขึ้นโดยใช้ประโยชน์จากเทคโนโลยีใหม่ๆ ที่สำคัญ การบริการโดยภาครัฐ (G-Services) ประกอบด้วย **บริการระบบคลาวด์ภาครัฐ (Government Cloud หรือ G-Cloud)** ทั้ง 3 รูปแบบดังนี้

- Software-as-a-Service (SaaS): คือแอปพลิเคชันภาครัฐต่างๆ ที่หน่วยงานสามารถใช้งานร่วมกันได้บนระบบคลาวด์ เช่น แอปพลิเคชันการจัดการข้อมูลอิเล็กทรอนิกส์ (Electronic Information Management) การจัดการ

ทรัพยากรมนุษย์ (Human Resources Management) และการจัดซื้อจัดจ้างทางอิเล็กทรอนิกส์ (Electronic Procurement) เป็นต้น

- Platform-as-a-Service (PaaS): คือแพลตฟอร์มสำเร็จรูปที่หน่วยงานภาครัฐสามารถใช้งานร่วมกันได้บนระบบคลาวด์ ในการพัฒนาแอปพลิเคชันต่างๆ โดยลดความยุ่งยากในการจัดเตรียมระบบพัฒนาแอปพลิเคชัน (Application Development Environment)
- Infrastructure-as-a-Service (IaaS): คือแพลตฟอร์มที่มีทรัพยากรการประมวลผลที่หน่วยงานภาครัฐสามารถใช้งานร่วมกันได้บนระบบคลาวด์ แพลตฟอร์มนี้สามารถขยายเพิ่มเติมได้ตามความต้องการและมีความยืดหยุ่น

นอกเหนือจากระบบคลาวด์ทั้ง 3 รูปแบบที่กล่าวมานั้น การบริการโดยภาครัฐ (G-Services) ยังรวมถึง**การบริการพื้นที่วางเครื่องแม่ข่าย (Colocation)** ของภาครัฐอีกด้วย

ในปัจจุบัน มีหน่วยงานภาครัฐไทยเพียง 16% ที่ใช้การบริการโดยภาครัฐ (G-Services) โดยมีการจัดเก็บ 9% ของปริมาณข้อมูลหน่วยงานทั้งหมดไว้กับการบริการนี้

ประโยชน์ของการบริการโดยภาครัฐ (G-Services) มีดังนี้

- ✓ *ประหยัดต้นทุน เนื่องจากข้อดีของการใช้พื้นที่จัดเก็บข้อมูลอย่างคุ้มค่า และมีการใช้ทรัพยากรร่วมกัน*
- ✓ *ประหยัดเวลาในการจัดซื้อ มีการดำเนินงานเชิงระบบที่ซับซ้อนน้อยลง และมีการให้บริการแบบ On-demand*
- ✓ *ยกระดับความสามารถในการรองรับการขยายบริการในอนาคต เพื่อตอบสนองความต้องการทรัพยากรและการบริการ IT ของหน่วยงานที่เปลี่ยนแปลงอย่างต่อเนื่อง*
- ✓ *กระตุ้นการจ้างงานและการบริการในสายอาชีพ IT ส่งเสริมการพัฒนาอุตสาหกรรม IT ในประเทศที่มีการสร้างเสริมทักษะวิชาชีพในด้านระบบคลาวด์*
- ✓ *มีโครงสร้างมาตรฐาน ระบบคลาวด์ และการสนับสนุนของภาครัฐ*
- ✓ *ยกระดับความปลอดภัย เนื่องจากการปฏิบัติตามมาตรฐานและการจัดเตรียมโครงสร้างพื้นฐานภาครัฐ*

แนวทางเชิงยุทธศาสตร์ที่สำคัญต่อหน่วยงานและภาครัฐ มีดังนี้

- ❖ หน่วยงานต้องเพิ่มปริมาณการจัดเก็บข้อมูลด้านความมั่นคงของประเทศ ข้อมูลสำคัญ และข้อมูลทั่วไปไว้กับการบริการโดยภาครัฐ (G-Services)
- ❖ หน่วยงานต้องดำเนินการสำรวจและศึกษาความเป็นไปได้ภายใต้โครงการ “iDiscover” เพื่อระบุข้อมูลที่สามารถจัดเก็บไว้กับ G-Services โดยมีระยะเวลาและแผนการดำเนินงานงาน รวมถึงจัดเตรียมรายละเอียดต่างๆ ตามแผนที่ได้กำหนดไว้
- ❖ หน่วยงานต้องดำเนินการศึกษาความเป็นไปได้ ในการจัดเก็บข้อมูลหรือแอปพลิเคชันใหม่ไว้กับ G-Services และต้องทำการจัดเก็บข้อมูลไว้กับ G-Services โดยที่หน่วยงานต้องส่งรายงานความเป็นไปได้และผลการดำเนินงานตามแผนที่ได้กำหนดไว้ ภายใต้โครงการ iDiscover
- ❖ ภาครัฐต้องดำเนินการศึกษาความเป็นไปได้ เพื่อเตรียมการดำเนินการบริการโดยภาครัฐ (G-Services) ในขั้นตอนต่อไป และต้องมีการจัดทำแผนความเป็นไปได้ ภายใต้โครงการ “iDiscover”

- ภาครัฐต้องสนับสนุนการปฏิบัติตามมาตรฐานที่กำหนดไว้สำหรับ G-Services ภายใต้โครงการ iAdopt ตามที่ระบุในเอกสารมาตรฐานบริการศูนย์ข้อมูลภาครัฐ (Government Data Center Service Standards)
- ภาครัฐต้องมีความพร้อมรองรับปริมาณข้อมูล สามารถรองรับการขยายตัวของบริการ และจัดการข้อมูลปริมาณมากในมุมมองของโครงสร้างพื้นฐาน โดยการเตรียมความพร้อมดังกล่าวสำหรับ G-Services เป็นการดำเนินงานส่วนหนึ่งของโครงการ “iTransform”
- หน่วยงานจะต้องพิจารณาเลือกใช้บริการ G-Services ในการจัดเก็บข้อมูลเป็นลำดับแรก ก่อนที่จะเลือกใช้บริการ 3rd Party Cloud หรือ Colocation หากกรณีที่ไม่เลือกใช้บริการจาก G-Services แทนการใช้บริการ 3rd Party Cloud หรือ Colocation นั้น หน่วยงานจะต้องส่งรายงานชี้แจงเหตุผลและความจำเป็น ซึ่งเป็นส่วนหนึ่งของโครงการ “iOptimize”
- หน่วยงานอาจต้องได้รับอนุญาตเพื่อใช้บริการคลาวด์ของหน่วยงานภายนอก (3rd Party Cloud) รายเดิม หากมีความต้องการที่เฉพาะเจาะจงเป็นพิเศษ หรือไม่มีผู้ให้บริการรายอื่นสามารถให้บริการได้ตามความต้องการ
- หน่วยงานต้องจัดเก็บข้อมูลทั่วไปชุดใหม่ไว้ก่อน และย้ายข้อมูลทั่วไปที่ความเหมาะสมไปเก็บไว้ที่ G-Services หลังจากทำการศึกษาความเป็นไปได้แล้ว โดยเป็นการดำเนินงานส่วนหนึ่งของโครงการ “iOptimize”

14. แนวทางปฏิบัติด้านเทคนิคของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐครอบคลุมแนวทางปฏิบัติด้านเทคนิคที่หน่วยงานต่างๆ ต้องปฏิบัติตาม เพื่อบริหารจัดการศูนย์ข้อมูลของตน แนวทางปฏิบัติด้านเทคนิคประกอบด้วย การดำเนินงานโดยอาศัยเทคโนโลยีและการดำเนินงานโดยอาศัยวิธีปฏิบัติที่เป็นเลิศ (Best Practice) เพื่อบริหารจัดการศูนย์ข้อมูล

การจัดการเครื่องแม่ข่าย (Server Management): คือการติดตามสถานะการทำงานของทรัพยากรที่สำคัญของระบบปฏิบัติการ เช่น หน่วยประมวลผล หน่วยความจำ และไฟล์ เป็นต้น นอกจากนี้ การจัดการเครื่องแม่ข่ายยังรวมถึง การกำหนดเกณฑ์ส่งสัญญาณเตือน (Warning Threshold) การผนวกเข้ากับ Enterprise Management System (EMS) และการออกแบบให้ทุกแพลตฟอร์มมีรูปแบบเดียวกัน

การจัดการฐานข้อมูล (Database Management): คือการติดตามสถานะการทำงานของทรัพยากรและตัวแปรสำคัญของฐานข้อมูล (Relational Database Management System หรือ RDBMS) แบบเชิงรุก เช่น Database Tables, Table Space และ Logs เป็นต้น นอกจากนี้ ควรมีการใช้ Enterprise Management System (EMS) และการบังคับใช้นโยบายที่เกี่ยวข้องควบคู่ไปด้วย

ระบบช่วยเหลือ (Helpdesk): คือการจัดเตรียมระบบช่วยเหลือกลางสำหรับศูนย์ข้อมูล ที่สำคัญ ระบบช่วยเหลือนี้ควรมีความสามารถให้ผู้ใช้งานบันทึกเหตุการณ์ (Incident) ได้ด้วยตนเองผ่านช่องทางต่างๆ โดยระบบช่วยเหลือจะสนับสนุนการรวบรวม จำแนกประเภท ติดตาม ยกระดับ และตรวจสอบเหตุการณ์และปัญหาทั้งหมดด้วย

การจัดการเครื่องแม่ข่ายเว็บ (Web Server Management): คือการติดตามสถานะการทำงานของ Web Server ซึ่ง Web Server จะถูกติดตามสถานะความพร้อมใช้งาน สภาพการทำงาน และประสิทธิภาพ

ความปลอดภัยของเครือข่าย (Network Security): คือการใช้งานระบบควบคุมการเข้าออกในอุปกรณ์เครือข่ายทั้งหมด โดยมีการควบคุมการเข้าออกระบบ (Access Control List) กลไกการยืนยันตัวบุคคล การตรวจจับการรุกล้ำ และการยืนยันตัวบุคคลด้วย Digital Certificate

การป้องกันไวรัส (Anti-Virus): คือมาตรการรักษาและระบบป้องกันไวรัสในศูนย์ข้อมูล โดยมีการตรวจสอบการรับส่งข้อมูลทั้งขาเข้าและขาออก รวมถึงบนระบบอีเมล์ทั้งหมด

ความปลอดภัยของเครื่องแม่ข่าย (Server Security): คือการใช้ระบบควบคุมพื้นฐานในเครื่องแม่ข่ายทุกเครื่องและระบบปฏิบัติการ เพื่อควบคุมการเข้าถึง (การยืนยันตัวบุคคลและการอนุญาต) เครื่องแม่ข่าย แพลตฟอร์ม และฐานข้อมูล โดยความปลอดภัยของเครื่องแม่ข่ายนี้ยังรวมถึงการทบทวนสิทธิการควบคุมการเข้าออก สิทธิการดูแลระบบ และความสามารถด้านความปลอดภัยให้ทันสมัย

การระบุตัวบุคคล การยืนยันตัวบุคคล และการอนุญาตตัวบุคคล (Identification, Authentication and Authorization): คือการจำกัดการเข้าถึงในรูปแบบอิเล็กทรอนิกส์ไปยังเว็บไซต์หรือแอปพลิเคชันที่นอกเหนือระดับของ

ผู้ใช้งานทั่วไป โดยที่จะมีการสงวนไว้ให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ระบบจะมีการระบุและยืนยันตัวบุคคล ที่สำคัญไม่อนุญาตให้ใช้รหัสผ่านที่สามารถคาดเดาได้ง่ายหรือการใช้รหัสผ่านร่วมกันในทุกกรณี

การจัดการรหัสผ่าน (Management of Password): คือการจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยมีการกำหนดแนวทางการปฏิบัติ เช่น การเปลี่ยนรหัสภายในจำนวนวันที่กำหนด การเข้ารหัสไฟล์ การตรวจสอบบัญชีผู้ใช้งาน และการตั้งรหัสผ่านที่ยากต่อการคาดเดา เป็นต้น

ความปลอดภัยในการรับส่งข้อมูล (Data Transmission Security): คือการปกป้องความลับและความสมบูรณ์ของข้อมูลทั้งหมดที่รับส่งผ่านเครือข่ายทุกรูปแบบ แนวปฏิบัตินี้แนะนำให้ใช้การเข้ารหัสระดับมาตรฐานอุตสาหกรรมสำหรับข้อมูลที่จัดอยู่ในประเภท “ชั้นความลับ”

การให้บริการ Firewall (Firewall Service): คือการบริหารจัดการให้บริการ Firewall ให้สอดคล้องกับข้อกำหนด นโยบายและกระบวนการของศูนย์ข้อมูล ได้แก่ การบำรุงรักษาทั่วไป การติดตามสถานะ และการเปลี่ยนแปลงกฎการใช้ Firewall เป็นต้น

การตรวจจับและป้องกันการรุกล้ำ (Intrusion Detection and Prevention Service): คือการใช้เครื่องมือตรวจจับและป้องกัน เพื่อตรวจจับการเข้าถึงหรือกิจกรรมที่มิได้รับอนุญาตในเครือข่าย ระบบคอมพิวเตอร์ และอุปกรณ์เครือข่ายที่เกี่ยวข้องกับศูนย์ข้อมูล

การติดตามสถานะความปลอดภัย (Security Monitoring): คือการติดตามสถานะความปลอดภัยศูนย์ข้อมูล โดยเฉพาะอย่างยิ่ง การติดตามสถานะระบบและอุปกรณ์เครือข่ายทั้งหมดแบบทันสถานการณ์ (Real-time) เพื่อตรวจจับการละเมิดความปลอดภัยที่อาจเกิดขึ้น

การตอบสนองเหตุการณ์ (Incident Response): คือการรายงานสถานการณ์ด้านการรักษาความปลอดภัยทั้งหมด โดยเฉพาะอย่างยิ่ง หน่วยงานต่างๆ จำเป็นต้องเก็บรักษารายการบันทึก (Log) ของระบบความปลอดภัยทั้งหมด เช่น Firewall ระบบตรวจจับการรุกล้ำ (IDS/IPS) มาตรการควบคุมการเข้าออก (ทั้งแบบอิเล็กทรอนิกส์และกายภาพ) และการบันทึกเพื่อตรวจสอบความสมบูรณ์ของไฟล์สำหรับตรวจสอบหรือใช้เป็นหลักฐาน

การสำรองข้อมูล (Backup): คือการสำรองข้อมูลแบบออนไลน์สำหรับแอปพลิเคชันที่สำคัญต่อพันธกิจไว้ที่ส่วนกลาง วิธีการสำรองข้อมูลควรมีให้เลือกใช้งานได้ในหลายระบบปฏิบัติการ สามารถรองรับการสำรองและกู้คืนข้อมูลด้วย SAN (Storage Area Network) จากแพลตฟอร์มต่างๆ ได้

การจัดการทรัพยากรจัดเก็บข้อมูล (Storage Resource Management): คือการจัดการและติดตามสถานะทรัพยากรของอุปกรณ์จัดเก็บข้อมูล SAN/NAS และรวมถึงการสำรวจโครงสร้างพื้นฐาน ระบบ File, Configuration Management, Event Management and Reporting และ Policy Management เป็นต้น

15. แนวทางปฏิบัติด้านนโยบายข้อมูลของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

แนวทางปฏิบัติด้านนโยบายข้อมูลของการพัฒนาศูนย์ข้อมูลภาครัฐ จะอธิบายถึงการบริหารของภาครัฐในการใช้งานข้อมูลร่วมกันอย่างมีประสิทธิภาพ ทันต่อเหตุการณ์ และมีความปลอดภัย เนื่องจากข้อมูลทั้งหมดที่ภาครัฐทำการรวบรวม จัดเก็บ จัดทำ ประมวลผล หรือใช้งานร่วมกัน เพื่อให้บริการและการดำเนินงานนั้นมีคุณค่าและประโยชน์ต่อประเทศ จึงจำเป็นต้องมีการป้องกันในระดับที่เหมาะสม ทั้งนี้การจำแนกประเภทความปลอดภัยบ่งบอกถึงความอ่อนไหวของข้อมูล (ในแง่ผลกระทบที่อาจเกิดขึ้น อันเป็นผลมาจากการรั่วไหล สูญหาย หรือการใช้ข้อมูลที่ผิดวิธี) และความจำเป็นที่ต้องปกป้องข้อมูลจากภัยคุกคามต่างๆ ข้อมูลสามารถจำแนกออกได้เป็น 3 ประเภท ดังนี้

ข้อมูลทั่วไป (Public Data)

ข้อมูลทั่วไปคือ ข้อมูลด้านการดำเนินงานภาครัฐและข้อมูลด้านการบริการของภาครัฐ ซึ่งข้อมูลประเภทนี้ครอบคลุมข้อมูลต่างๆ ที่มีคุณค่าและความอ่อนไหวที่แตกต่างกัน จึงจำเป็นต้องมีการป้องกันจากภัยคุกคาม และต้องปฏิบัติตามกฎหมาย ข้อบังคับ และพันธะในระดับสากล ดังนี้

- ✓ ข้อมูลการดำเนินงานตามภารกิจของภาครัฐประจำวัน การให้บริการของภาครัฐ และการคลังสาธารณะ
- ✓ ข้อมูลการดำเนินความสัมพันธ์ระหว่างประเทศและกิจกรรมทางการทูตประจำวัน
- ✓ ข้อมูลความปลอดภัยสาธารณะ กระบวนการยุติธรรมทางอาญา และการบังคับใช้กฎหมาย
- ✓ ข้อมูลผลประโยชน์ทางการค้า
- ✓ ข้อมูลประชาชนทั่วไป ที่ไม่รวมถึงข้อมูลที่มีความอ่อนไหว เช่น เลขประจำตัวบัตรประชาชน เลขที่หนังสือเดินทาง หรือข้อมูลส่วนบุคคลเป็นต้น

ข้อมูลสำคัญ (Important Data)

ข้อมูลสำคัญคือ ข้อมูลที่มีความอ่อนไหวที่ต้องได้รับการปกป้องจากภัยคุกคามที่มีศักยภาพสูง และหากเกิดการโจมตีหรือรั่วไหลของข้อมูลโดยเจตนาหรือไม่ก็ตาม จะส่งผลกระทบดังต่อไปนี้

- ✓ คุกคามอิสรภาพหรือความปลอดภัยของประชาชนโดยตรง
- ✓ สร้างความเสียหายต่อประสิทธิภาพการดำเนินงานของประเทศ
- ✓ สร้างความเสียหายต่อประสิทธิภาพการปฏิบัติงานการข่าวกรอง
- ✓ ก่อความเสียหายอย่างใหญ่หลวงต่อความสามารถในการสืบสวนสอบสวนหรือดำเนินคดีอาชญากรรมร้ายแรง

ข้อมูลด้านความมั่นคงของประเทศ (National Security Data)

ข้อมูลด้านความมั่นคงของประเทศ คือข้อมูลที่มีความอ่อนไหวสูงสุดที่มีทั้งประโยชน์และผลกระทบต่อความมั่นคงของประเทศหรือชาติพันธมิตร ที่ต้องได้รับการป้องกันในระดับสูงสุดจากภัยคุกคามรูปแบบต่างๆ และหากเกิดการโจมตีหรือรั่วไหลของข้อมูลโดยเจตนาหรือไม่ก็ตาม จะส่งผลกระทบดังต่อไปนี้

- ✓ นำไปสู่การสูญเสียชีวิตในวงกว้างโดยตรง

- ✓ คุกคามเสถียรภาพภายในประเทศโดยตรง
- ✓ เพิ่มภาวะความตึงเครียดระหว่างประเทศ
- ✓ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อประสิทธิภาพหรือความมั่นคงของประเทศ
- ✓ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อความสัมพันธ์ระหว่างประเทศที่เป็นมิตรอันดีต่อกัน
- ✓ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อประสิทธิภาพการปฏิบัติการความมั่นคงหรืองานข่าวกรองในระดับสูงสุด
- ✓ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อความมั่นคงและการฟื้นฟูสภาพทรัพย์สินอันเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical National Infrastructure)

การจำแนกข้อมูลดังที่กล่าวมาข้างต้นกำหนดบรรทัดฐานในการควบคุมความปลอดภัยส่วนบุคคล ความปลอดภัยทางกายภาพ และความปลอดภัยของข้อมูล โดยมีระดับการคุ้มครองจากภัยคุกคามอย่างเหมาะสม ข้อมูลทั้งหมดต้องมีการจัดการอย่างรอบคอบให้สอดคล้องกับกฎหมายและข้อบังคับ เพื่อลดความเสี่ยงจากการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต นอกจากนี้ หน่วยงานต่างๆ อาจต้องประยุกต์ใช้มาตรการควบคุมข้างต้นในการจัดการความเสี่ยงให้เหมาะสมกับสถานการณ์และสอดคล้องกับระดับความเสี่ยงที่ภาครัฐยอมรับได้ (Government Risk Appetite Tolerance) การจำแนกนี้ใช้ได้กับข้อมูลหรือทรัพย์สินอื่นที่มีความเฉพาะตัว นอกจากนี้ โครงสร้างพื้นฐาน ICT สำคัญ (เช่น ชุดข้อมูลขนาดใหญ่ ระบบการจ่ายเงิน เป็นต้น) อาจต้องมีมาตรการควบคุมเพิ่มเติม เพื่อจัดการชั้นความลับ ความสมบูรณ์ และความเสี่ยงด้านความพร้อมใช้งาน โดยการประเมินความเสี่ยงจะตัดสินเป็นรายกรณีไป

16. แนวทางปฏิบัติด้านนโยบายการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

พฤติกรรมภายในศูนย์ข้อมูล (Behavior in Data Center)

เจ้าหน้าที่และผู้เกี่ยวข้องที่เข้าออกศูนย์ข้อมูลต้องปฏิบัติตัวอย่างเหมาะสม ไม่ทำความเสียหายต่อโครงสร้างพื้นฐาน ไม่พกพาวัตถุไวไฟหรือที่เป็นอันตราย แต่งกายสุภาพเหมาะสม ปฏิบัติตามคำแนะนำของเจ้าหน้าที่และกฎระเบียบอย่างเคร่งครัด หากมีการตรวจค้น หรืออยู่ภายใต้สถานการณ์ฉุกเฉินต่างๆ

การภาพถ่ายหรือวิดิทัศน์ (Pictures or Video)

ห้ามบุคคลใดทำการถ่ายภาพ ถ่ายวิดิทัศน์ รวมถึงการบันทึกเสียงทุกประเภทในศูนย์ข้อมูล

ความปลอดภัยทางกายภาพ (Physical Security)

ศูนย์ข้อมูลต้องจำกัดการเข้าออก ต้องมีเจ้าหน้าที่รักษาความปลอดภัยประจำการที่ศูนย์ข้อมูลตลอดเวลา 24 ชั่วโมง 7 วันต่อสัปดาห์ ต้องติดตั้งกล้องรักษาความปลอดภัย และควรจำกัดการเข้าออกในพื้นที่สำคัญ

การเข้าออกศูนย์ข้อมูล (Data Center Ingress and Egress)

ผู้มาติดต่อจะสามารถเข้าสู่ศูนย์ข้อมูลได้หากได้รับอนุญาตแล้วเท่านั้น โดยต้องมีบัตรประจำตัวที่เจ้าหน้ารับผิดชอบศูนย์ข้อมูลเป็นผู้ออกให้และได้รับการอนุญาตให้เข้าออกอาคารได้

การจัดการสิทธิในการเข้าถึงทรัพยากร (Access List Management)

แนวทางปฏิบัตินี้กำหนดให้กระทรวงและหน่วยงานต่างๆ มีหน้าที่ดูแลรักษา และปรับปรุงสิทธิในการเข้าถึงทรัพยากรในศูนย์ข้อมูล

พื้นที่ส่วนกลาง (Common Area)

แนวทางปฏิบัตินี้ระบุข้อกำหนดการใช้พื้นที่ส่วนกลางภายในศูนย์ข้อมูล ซึ่งบุคลากรต้องใช้พื้นที่ส่วนกลางอย่างเหมาะสม

ข้อกำหนดการติดตั้งกรงและตู้ และการเดินสายสัญญาณ (Cage, Cabinet and Cabling Requirements)

แนวทางปฏิบัตินี้เกี่ยวข้องกับการจัดการตู้ภายในศูนย์ข้อมูล ซึ่งกำหนดรายละเอียดด้านความปลอดภัย ความสะอาด และการทิ้งวัสดุเหลือใช้ นอกจากนี้ แนวทางปฏิบัติห้ามมิให้สร้างพื้นที่สำนักงานใกล้บริเวณตู้ ห้ามนำวัสดุไวไฟเข้าใกล้ตู้ ห้ามวางสิ่งของบนตัวตู้ ห้ามทำการดัดแปลงพื้นที่ตู้ และห้ามวางอุปกรณ์ไว้นอกตู้

แร็คและประตูตู้ (Rack/Cabinet Doors)

ห้ามมิให้บุคคลใดถอดหรือเปลี่ยนประตูตู้ หรือหากจำเป็นจะต้องได้รับการอนุญาตก่อนเท่านั้น

กระเบื้องปูพื้น (Floor Tiles)

ห้ามมิให้บุคคลใดยกหรือเคลื่อนย้ายกระเบื้องปูพื้น นอกจากผู้ได้รับการอนุญาตเท่านั้นถึงจะดำเนินการได้

อุปกรณ์ศูนย์ข้อมูล (Data Center Equipments)

การให้ผู้ใช้บริการยืมอุปกรณ์จากศูนย์ข้อมูลนั้น หน่วยงานที่อนุญาตต้องเป็นผู้รับผิดชอบต่ออุปกรณ์นั้น

การรับอุปกรณ์ (Receiving)

การรับอุปกรณ์ในศูนย์ข้อมูลนั้นมีการระบุว่าอุปกรณ์ทั้งหมดในศูนย์ข้อมูลควรมีการรับมอบบริเวณจุดรับของ (Receiving Dock) เท่านั้น โดยต้องระบุชื่อหน่วยงานและผู้รับผิดชอบกำกับไว้ด้วย

การขนย้ายอุปกรณ์เมื่อสิ้นสุดสัญญาการให้บริการ (Removal of Equipment at End of Term)

หน่วยงานต้องดำเนินการขนย้ายอุปกรณ์ฮาร์ดแวร์ออกจากศูนย์ข้อมูลภายในระยะเวลาวันสิ้นสุดสัญญาการให้บริการ (Effective Cancellation Date)

รางปลั๊กของผู้ใช้บริการ (User Provided Power Strips)

ข้อกำหนดนี้ห้ามหน่วยงานเพิ่มรางปลั๊กที่ศูนย์ข้อมูลเองในทุกกรณี

การเพิ่มอุปกรณ์รักษาความมั่นคงปลอดภัยที่เป็นของผู้ใช้บริการ (User Provided Additional Security Devices)

แนวทางปฏิบัตินี้ระบุข้อกำหนดการเพิ่มอุปกรณ์รักษาความปลอดภัย ซึ่งไม่อนุญาตให้หน่วยงานเพิ่มอุปกรณ์รักษาความปลอดภัย ที่อาจสร้างความลำบากในการเข้าถึงตู้ของตนเอง เช่น การนำกุญแจตู้มาติดตั้งเพิ่มเติม เป็นต้น

17. แนวทางปฏิบัติด้านการเงินของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

หนึ่งในเป้าหมายหลักของยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ คือการเพิ่มประสิทธิภาพต้นทุนที่ต้องใช้จ่ายตลอดอายุการทำงานของโครงสร้างพื้นฐานด้านข้อมูล ซึ่งการเพิ่มประสิทธิภาพต้นทุนภายใต้กรอบของยุทธศาสตร์ มีดังต่อไปนี้

เพิ่มประสิทธิภาพการใช้งานโครงสร้างพื้นฐานด้านข้อมูล
ลดการใช้พื้นที่ศูนย์ข้อมูลและต้นทุนที่เกี่ยวข้อง
เพิ่มประสิทธิภาพการใช้ทรัพย์สินด้าน ICT ของศูนย์ข้อมูล
ยกระดับโครงสร้างพื้นฐานด้าน ICT ของศูนย์ข้อมูลให้สอดคล้องกับความต้องการในการดำเนินงาน
สถาปัตยกรรมโครงสร้างพื้นฐานด้าน ICT ที่ได้มาตรฐานและมีการใช้งานเทคโนโลยีใหม่เร็วขึ้น
การระบุประเภทข้อมูล การย้ายไปใช้วิธีจัดเก็บข้อมูลที่เหมาะสม และการใช้ประโยชน์ข้อมูลอย่างคุ้มค่า

การพัฒนาโครงสร้างศูนย์ข้อมูลกลายเป็นปัจจัยสำคัญต่อความสามารถในการแข่งขัน การพัฒนาโครงสร้างศูนย์ข้อมูลจะเป็นยุทธศาสตร์สำคัญที่เพิ่มประสิทธิภาพการให้บริการแก่ประชาชนหากมีการดำเนินการอย่างเหมาะสม อย่างไรก็ตาม การพัฒนาดังกล่าวมีค่าใช้จ่ายซึ่งจำเป็นต้องมีการปรับสมดุลระหว่างความเสี่ยงและผลตอบแทนภายใต้งบประมาณที่ได้รับ นอกจากนี้ระดับความเสี่ยงไม่เพียงขึ้นอยู่กับความทันสมัยของอุปกรณ์ หากยังรวมถึงความสามารถของบุคลากรที่ดูแลอุปกรณ์เหล่านั้นด้วย ศูนย์ข้อมูลจำเป็นต้องมีการปรับปรุงเพื่อรองรับเป้าหมายของหน่วยงานภาครัฐที่เปลี่ยนไป โดยเฉพาะอย่างยิ่งศูนย์ข้อมูลที่มีการใช้งานมานานนั้นควรต้องดำเนินการปรับปรุงในด้านต่างๆ เช่น ความเพียงพอของพื้นที่ศูนย์ข้อมูล ระบบทำความเย็นที่ขาดประสิทธิภาพ และโครงสร้างพื้นฐานด้านไฟฟ้าไม่เหมาะสมต่อการขยายตัวของบริการ เป็นต้น นอกจากนี้ ศูนย์ข้อมูลควรได้รับการประเมินเพื่อพิจารณาว่ามีค่าใช้จ่ายในการดูแลรักษาที่สูงเกินไปหรือไม่ หรือระบบที่ใช้งานมานานส่งผลต่อเสถียรภาพการดำเนินงานของศูนย์ข้อมูลหรือไม่

การพัฒนาศูนย์ข้อมูลมีผลตอบแทนทางการเงินอย่างชัดเจน ซึ่งผลตอบแทนดังกล่าวสามารถประเมินได้จากหลายวิธีดังต่อไปนี้

- การลดจำนวนศูนย์ข้อมูลช่วยประหยัดค่าใช้จ่ายที่สิ้นเปลือง ประหยัดต้นทุนการดำเนินงานที่เกี่ยวกับสถานที่ตั้งศูนย์ข้อมูล และช่วยประหยัดค่าใช้จ่ายด้านพลังงานของศูนย์ข้อมูล
- การผนวกซอฟต์แวร์ไว้บนแพลตฟอร์มเดียวกัน จะส่งผลให้ฮาร์ดแวร์มีจำนวนลดลง ซึ่งช่วยประหยัดค่าใช้จ่ายในการซ่อมบำรุงฮาร์ดแวร์และค่าลิขสิทธิ์ซอฟต์แวร์
- การพัฒนาศูนย์ข้อมูลช่วยลดจำนวนเครื่องแม่ข่าย ระบบจัดเก็บข้อมูล และอุปกรณ์เครือข่ายที่ต้องจัดซื้อ ซึ่งส่งผลให้มีต้นทุนการจัดซื้อและค่าใช้จ่ายต่ำลง
- การใช้งานแอปพลิเคชันร่วมกัน เช่น ระบบการจัดซื้อ การจัดการสินค้าคงคลัง การออกใบแจ้งหนี้ หรือรายงานการบริหารจัดการ เป็นต้น ส่งผลให้การอัพเกรดแอปพลิเคชันเหล่านี้สามารถทำได้ง่ายขึ้น และประหยัดค่าใช้จ่าย
- การพัฒนาศูนย์ข้อมูลลดความซับซ้อนและข้อผิดพลาดในกระบวนการเชิงระบบ เช่น การรักษาความปลอดภัยข้อมูล การบริการเครือข่าย การรักษาความปลอดภัย และการบริหารจัดการระบบ

- การพัฒนาศูนย์ข้อมูลยังช่วยตรวจสอบกระบวนการดำเนินงาน ปรับเปลี่ยนบทบาทหน้าที่และกระบวนการให้เหมาะสมต่อทรัพยากรที่ใช้ในการประมวลผลและบุคลากรด้าน IT

การพัฒนาศูนย์ข้อมูลภาครัฐของไทยเป็นโครงการที่มีลักษณะพิเศษ เนื่องจากเกี่ยวข้องกับโครงสร้างพื้นฐานภาครัฐขนาดใหญ่ในรูปแบบของศูนย์ข้อมูลระดับหน่วยงานที่ภาครัฐได้มีการลงทุนในช่วงที่ผ่านมาไม่นานนัก

ตามที่ได้กล่าวมา ประโยชน์ของโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) สำหรับประเทศไทยนั้นมีหลายประการซึ่งจะเห็นผลไปอย่างต่อเนื่อง คุณประโยชน์สำคัญประกอบด้วย ดังนี้

	การลงทุน	ประโยชน์ที่ได้รับ
การนำมาตรฐานมาใช้	การนำมาตรฐานมาใช้ต้องอาศัยการลงทุนที่สูง ซึ่งแต่ละหน่วยงานต้องดำเนินงานให้สอดคล้องกับมาตรฐานที่กำหนด	ระบบที่ดำเนินการตามมาตรฐานในระดับสูงจะลดความซ้ำซ้อนและการสูญหายของข้อมูล ส่งผลให้ข้อมูลมีความถูกต้องและสมบูรณ์ มีบริการที่รวดเร็ว และมีประสิทธิภาพโดยรวมเชิงระบบของหน่วยงานและภาครัฐ นอกจากนี้ การนำมาตรฐานมาใช้อาจส่งผลให้เกิดประโยชน์ในด้านการเงิน เนื่องจากเวลาดำเนินงานที่ลดลง การประมวลผลและการจัดเก็บข้อมูลที่มีประสิทธิภาพ ย่อมส่งผลให้เกิดการประหยัดค่าใช้จ่ายอย่างแน่นอน การนำมาตรฐานมาใช้ยังช่วยประหยัดต้นทุน เช่น ค่าไฟฟ้า ค่าบริการ ค่าซ่อมบำรุง และทรัพยากรบุคคล เป็นต้น
การปฏิบัติตามข้อกำหนดด้านความปลอดภัย	การปฏิบัติตามข้อกำหนดด้านความปลอดภัยส่งผลให้เกิดความจำเป็นในการจำแนกประเภทข้อมูลแล้วนำไปบริหารจัดการอย่างเหมาะสม ซึ่งอาจส่งผลให้เกิดการลงทุนเพื่อย้ายข้อมูลไปยังระบบที่มีการบริหารจัดการที่มีความเหมาะสมกับประเภทของข้อมูลนั้นๆ	มูลค่าความเสียหายอาจเกิดขึ้น หากข้อมูลที่จัดเก็บไว้เกิดสูญหายหรือรั่วไหล ความสูญเสียจากการไม่ปฏิบัติตามข้อกำหนดด้านความปลอดภัยอาจมีมูลค่าสูง หรือไม่อาจประเมินมูลค่าได้ ดังนั้นการปฏิบัติตามข้อกำหนดนี้ส่งผลให้ความเสี่ยงในการสูญเสียข้อมูลอันมีค่าลดลงไปด้วยเช่นกัน
การเพิ่มประสิทธิภาพพื้นที่จัดเก็บข้อมูล	การดำเนินงานตามมาตรฐานจะช่วยเพิ่มประสิทธิภาพพื้นที่จัดเก็บข้อมูล	พื้นที่จัดเก็บข้อมูลที่เพิ่มขึ้นจากการบริหารจัดการอย่างมีประสิทธิภาพจะลดความต้องการในการจัดซื้อฮาร์ดแวร์ใหม่
การเพิ่มการใช้ประโยชน์ทรัพยากรภาครัฐ	GDCM จะส่งผลให้มีการใช้งานทรัพยากรภาครัฐในอัตราที่สูงขึ้น อันเป็นผลจากการย้ายข้อมูล ลดจำนวนหรือปิดศูนย์ข้อมูล และเพิ่มประสิทธิภาพการบริการ ซึ่งการบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) หรือการบริการโดยภาครัฐ (G-Services) นับเป็น	อัตราการใช้งานที่สูงขึ้นจะลดต้นทุนการดำเนินงานและค่าใช้จ่ายในการลงทุน ซึ่งทำให้เกิดผลตอบแทนจากการลงทุนสูงขึ้น

	การลงทุน	ประโยชน์ที่ได้รับ
	ทางเลือกเพิ่มเติม โดยทางเลือกทั้งหมดนี้ต้องอาศัยการลงทุนจากภาครัฐ	
การเพิ่มประสิทธิภาพด้านต้นทุน	วิธีการจัดเก็บข้อมูลที่หลากหลายนำไปสู่การให้บริการร่วมกันแบบใหม่ โดยอาศัยการบริการโดยภาครัฐ ศูนย์ข้อมูลระดับกระทรวง และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน ซึ่งจะลดการพึ่งพางบประมาณการลงทุน แต่อาจเพิ่มค่าใช้จ่ายในการดำเนินงาน	ผลตอบแทนจากการลงทุนจะเพิ่มขึ้นอย่างมีนัยสำคัญ เนื่องจากหน่วยงานจะมีภาระในการดูแลทรัพย์สินน้อยลง และมุ่งเน้นการให้บริการในต้นทุนที่ต่ำลงจากการเจรจาต่อรอง
การมุ่งเน้นภารกิจหลัก	หน่วยงานที่จัดจ้างหน่วยงานภายนอกเพื่อรองรับความต้องการด้านข้อมูลจะใช้ต้นทุนในการดำเนินงานสูงขึ้น แต่จะเป็นการใช้จ่ายงบประมาณอย่างคุ้มค่า	หน่วยงานสามารถมุ่งเน้นหน้าที่ตามภารกิจหลักโดยสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพมากขึ้นและเพิ่มผลตอบแทนจากการลงทุนได้สูงขึ้น
การถ่ายโอนทรัพยากรบุคคล	ภายใต้การจัดเก็บข้อมูลที่มีให้เลือกในหลายรูปแบบ ทรัพยากรบุคคลที่มีจำกัดของหน่วยงานนั้น จะมีการใช้งานร่วมกันระหว่างหน่วยงานและการบริการอื่น	สามารถลดต้นทุนด้านการบริหารจัดการทรัพยากรบุคคลได้ในระยะยาว

18. แผนการดำเนินงานการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM Strategy) มีการแบ่งการดำเนินงานเป็นหลายระยะในช่วงระยะเวลา 5 ปี (ค.ศ. 2018 - 2022) เนื่องจากหน่วยงานภาครัฐต่างๆ จะมีการพัฒนาและปรับเปลี่ยนโครงสร้างเทคโนโลยีสารสนเทศของตนเพื่อรองรับการดำเนินงานรูปแบบใหม่ การมียุทธศาสตร์และการดำเนินงานในทิศทางเดียวกันมีบทบาทสำคัญในการขับเคลื่อนการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ให้ประสบผลสำเร็จ การดำเนินงานที่สำคัญที่จะเกิดขึ้นในช่วงระยะเวลา 5 ปีได้แก่ การทำสัญญาจ้างหน่วยงานภายนอก การจ้างบุคลากร การกำหนดเวลาในการทดแทนทรัพย์สิน (Asset Refreshment Cycle) การเช่าซื้อบริการซ่อมบำรุง การปลดระวางศูนย์ข้อมูลหรือทรัพย์สิน การขยายพื้นที่จัดเก็บข้อมูลของศูนย์ข้อมูล การจัดเตรียมงบประมาณลงทุน เป็นต้น ดังนั้นหน่วยงานและกระทรวงต่างๆ จึงจำเป็นต้องมีความเข้าใจในแนวทางการดำเนินงานที่ตรงกัน

แผนการดำเนินงานการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) กำหนดแนวทางการดำเนินงานในภาพรวมให้แก่หน่วยงานภาครัฐสำหรับระยะเวลา 5 ปี (ค.ศ. 2018 - 2022) ทั้งนี้ หน่วยงานต้องแสดงแผนการดำเนินงานและผลลัพธ์ที่คาดหวังไว้ในแผนยุทธศาสตร์เป็นรายหน่วยงานสำหรับปีที่ 1 ของการพัฒนาศูนย์ข้อมูลภาครัฐ นอกจากนี้ แผนยุทธศาสตร์รายหน่วยงานนั้นยังต้องสอดคล้องกับยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐอีกด้วย โดยในช่วง 5 ปี ของยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) มุ่งตอบสนองวัตถุประสงค์ต่อไปนี้

- ✓ รวบรวมความต้องการศูนย์ข้อมูลทั้งหมด และดำเนินการศึกษาความเป็นไปได้ เพื่อขับเคลื่อนยุทธศาสตร์ GDCM
- ✓ ระบุและจัดทำข้อกำหนดสำหรับรูปแบบการดำเนินงานในอนาคต
- ✓ ช่วยเหลือหน่วยงานนำร่องในการย้ายไปสู่การใช้ทรัพยากรร่วมกัน
- ✓ นำมาตรฐานมาประยุกต์ใช้กับการดำเนินงานศูนย์ข้อมูล เพื่อให้เกิดประสิทธิภาพสูงสุด
- ✓ จัดทำรูปแบบการใช้บริการร่วมกัน (Shared Services Model)
- ✓ หน่วยงานนำแผนงานไปปฏิบัติ
- ✓ เผยแพร่พัฒนาการและความก้าวหน้าของโครงการ

ปัจจัยขับเคลื่อนการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ตัวชี้วัดประสิทธิภาพ	ปัจจัยขับเคลื่อนยุทธศาสตร์
การใช้งานทรัพย์สินและพื้นที่จัดเก็บข้อมูล	■ ความมุ่งมั่นและความรับผิดชอบต่อการเพิ่มอัตราการใช้งานอย่างแท้จริง โดยอาศัยรูปแบบการดำเนินงานในอนาคตที่มีให้เลือกใช้งาน ■ การลงทุนทั้งเวลาและความพยายามในการเพิ่มความสามารถของศูนย์ข้อมูลเพื่อเพิ่มอัตราการใช้งาน กำหนดขั้นตอนในการเพิ่มคุณค่าทรัพย์สินและประสิทธิภาพ โดยการประยุกต์ใช้มาตรฐาน
การพัฒนาบุคลากร	■ ภาครัฐจัดทำแผนฝึกอบรม เพื่อพัฒนาคุณภาพและประสิทธิภาพของบุคลากร ■ หน่วยงานเปิดกว้างและสนับสนุนบุคลากรด้วยการฝึกอบรม ตั้งแต่การจัดหาหลักสูตร พัฒนาหลักสูตร การฝึกอบรม และพัฒนาทักษะอย่างต่อเนื่อง ■ การหมุนเวียนบุคลากรของหน่วยงาน เพื่อใช้ประโยชน์จากบุคลากรที่มีอยู่เดิมอย่างมีประสิทธิภาพ ตลอดจนสามารถใช้ประโยชน์จากทรัพยากรบุคคลในการดำเนินงานรูปแบบอื่นๆ เช่น การบริการโดยภาครัฐ ศูนย์ข้อมูลระดับกระทรวง และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน
การบริการร่วมกัน	■ จัดตั้งเจ้าหน้าที่กำกับดูแลการดำเนินงาน (Governance Committee) เพื่อติดตามสถานะการใช้บริการร่วมกัน โดยหน่วยงานมีภาระรับผิดชอบในการใช้บริการร่วมกันตามแผนที่กำหนดไว้ ■ พัฒนาความสามารถ คุณภาพ มาตรฐาน ความสามารถในการรองรับการขยายตัวของบริการ และการจัดเตรียมรูปแบบทางเลือกของการบริการร่วมกันตามที่กำหนดไว้ ■ มีการศึกษาความเป็นไปได้อย่างเหมาะสมในมุมมองของหน่วยงาน เพื่อระบุข้อมูลที่สามารถใช้งานร่วมกัน
การเพิ่มประสิทธิภาพต้นทุน	■ หน่วยงานต้องเพิ่มประสิทธิภาพต้นทุน โดยอาศัย 6 รูปแบบการดำเนินงานในอนาคตเพื่อตอบสนองความต้องการด้านข้อมูล ■ ปรับกระบวนการและแผน เพื่อลดการพึ่งพางบประมาณลงทุนและค่าใช้จ่ายในการดำเนินงานของภาครัฐ ■ ดำเนินการประเมินงบประมาณในปีที่ 1 เพื่อระบุ ตรวจสอบ และประมาณการ งบประมาณทั้งหมดที่สามารถประหยัดได้ จากการดำเนินงานตามโครงการ GDCM
ความปลอดภัย	■ กำหนดแนวทางยกระดับสถานะการรักษาความปลอดภัยของหน่วยงานให้สอดคล้องกับโครงการที่กำลังดำเนินงาน แอปพลิเคชัน และการจัดเก็บข้อมูลในปัจจุบัน ■ หน่วยงานดำเนินการวิเคราะห์ความเป็นไปได้ เพื่อกำหนดสถานะความปลอดภัย ความเสี่ยง และกำหนดแผนบรรเทาความเสี่ยงให้สอดรับกับแนวทางปฏิบัติด้านความปลอดภัย
กรอบยุทธศาสตร์	■ ยุทธศาสตร์ GDCM เป้าหมายหลัก นโยบายภาครัฐ และผลลัพธ์ ที่จะจัดทำขึ้นในปีที่ 1 มีกรอบที่ชัดเจน ■ กำหนดโครงสร้างองค์กรที่เน้นการดำเนินงานยุทธศาสตร์ ตลอดจนติดตามสถานะความก้าวหน้า

หลักการในการกำหนดแนวทางดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

หลักการในการกำหนดแนวทางดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ถูกจัดทำขึ้นเพื่อกำหนดทิศทาง สนับสนุนการออกแบบ และสนับสนุนการดำเนินงานตั้งแต่ระยะที่ 1 ของแผนการดำเนินงาน ที่จะสนับสนุนการดำเนินงานของภาครัฐ หน่วยงาน และกระทรวงต่างๆ ให้ก้าวผ่านการเปลี่ยนแปลงจากสถานะปัจจุบัน (As-Is) ไปสู่สถานะเป้าหมาย (To-Be)

หลักการในการกำหนด		นัยในการกำหนดแนวทางดำเนินงาน
ความรับผิดชอบ	มีความเป็นเจ้าของและความรับผิดชอบที่ชัดเจนทั่วทั้งระบบและภายในกระบวนการตั้งแต่ต้นจนจบ	■ ความรับผิดชอบสำหรับระบบตั้งแต่ต้นจนจบอยู่ในอำนาจหน้าที่ของภาครัฐหรือหน่วยงานใดหน่วยงานหนึ่งทั้งหมด ■ ต้องกำหนดความรับผิดชอบของหน่วยงาน ความรับผิดชอบของบุคลากร ความรับผิดชอบของภาครัฐ หรือความรับผิดชอบของฝ่ายบริหาร ■ ความรับผิดชอบที่ชัดเจนจะผลักดันประสิทธิภาพรายบุคคลและบุคลากรทั้งคณะ
การเติบโตของประเทศ	มีศักยภาพที่จะสนับสนุนและขับเคลื่อนการเติบโตของประเทศ ในด้านการบริการประชาชน ข้อมูล คุณภาพ ความก้าวหน้าทางเทคโนโลยี และเศรษฐกิจดิจิทัล	■ พัฒนาศักยภาพของประเทศไทย เพื่อส่งเสริมและสนับสนุนการเติบโตของประเทศ ■ มอบอำนาจให้หน่วยงานคัดสรรทางเลือกที่เหมาะสมที่สุดจาก 6 รูปแบบการดำเนินงานในอนาคต ตามแนวทางปฏิบัติที่กำหนดไว้ ■ ฝึกอบรมและเตรียมบุคลากรให้พร้อมสำหรับการเปลี่ยนแปลง ■ มุ่งพัฒนาประเทศสู่การเป็นศูนย์กลางทางเทคโนโลยี เพื่อให้พร้อมรองรับปริมาณข้อมูลที่เพิ่มขึ้น
ศักยภาพ	มุ่งเน้นการใช้จุดแข็งและสร้างศักยภาพทั่วทั้งระบบ เพื่อสร้างประโยชน์ให้เกิดอย่างเป็นรูปธรรม	■ สร้างศูนย์ความเป็นเลิศ เพื่อมุ่งเน้นการฝึกอบรมและการเรียนรู้ ■ ภาครัฐต้องระบุหน่วยงานนำร่องในการดำเนินงานรูปแบบในอนาคต เพื่อเป็นต้นแบบสำหรับการเปลี่ยนแปลง ■ ระบุจุดอ่อนทางศักยภาพและสร้างโครงสร้างพื้นฐานของภาครัฐ เพื่อสนับสนุนการพัฒนาศักยภาพ ■ การบูรณาการและการจำแนกประเภทข้อมูลเป็นกระบวนการสำคัญที่จะทำให้เกิดการใช้พื้นที่จัดเก็บข้อมูลอย่างมีประสิทธิภาพ บทบาทและความรับผิดชอบที่ชัดเจน การประหยัดพื้นที่ และลดความซ้ำซ้อนของข้อมูล
นวัตกรรม	สนับสนุนนวัตกรรม และใช้เทคโนโลยีประสิทธิภาพสูง เพื่อส่งเสริมอัตราการเติบโตทางนวัตกรรม	■ รักษาและคงไว้ซึ่งจุดแข็งและความสามารถหลักที่มีอยู่ในปัจจุบันของหน่วยงาน เช่น ระบบคอมพิวเตอร์ และแอปพลิเคชัน เป็นต้น หากโครงสร้างพื้นฐานใหม่ยังไม่สามารถให้บริการได้ ■ จัดตั้งการบริการร่วมกัน ตั้งแต่ระดับหน่วยงาน กระทรวง และระหว่างหน่วยงาน โดยใช้องค์ประกอบของมาตรฐานต่างๆ เพื่อพัฒนาและขยายโครงสร้างพื้นฐาน ■ พัฒนาการบริการโดยภาครัฐ (G-Services) และเพิ่มสัดส่วนการใช้บริการคลาวด์ให้มากขึ้น ■ สนับสนุนวัฒนธรรมสร้างสรรค์นวัตกรรม เพื่อให้มีแนวทางในการรองรับความเสี่ยงที่อาจเกิดขึ้น และการพัฒนาในอนาคต

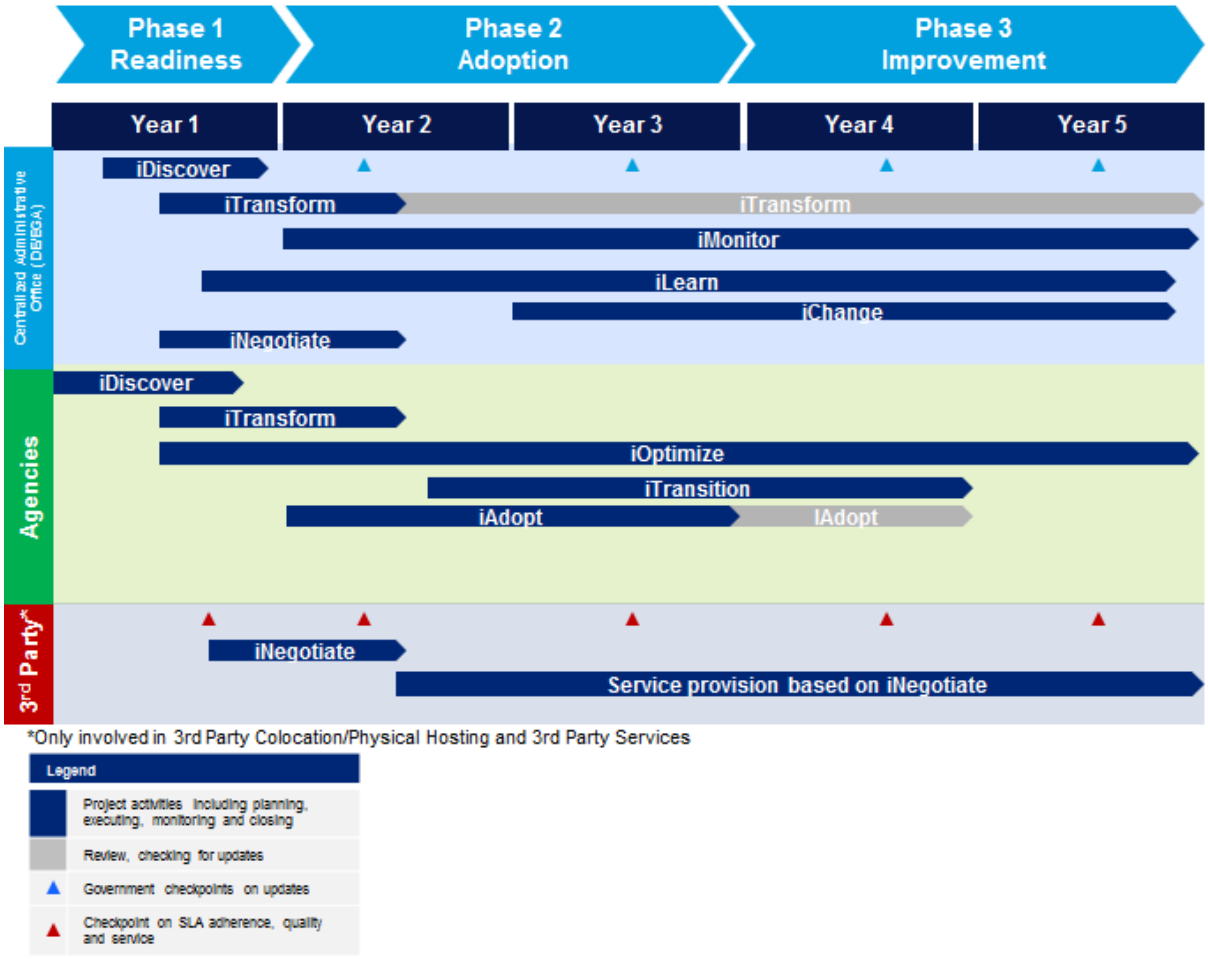
หลักการการออกแบบ		นัยสำคัญในการออกแบบองค์กร
การร่วมมือกัน	จัดทำโครงสร้างที่สนับสนุนการทำงานร่วมกันและมีประสิทธิภาพระหว่างหน่วยงาน	▪ ใช้ประโยชน์จากวัฒนธรรมการทำงานร่วมกัน เพื่อเพิ่มประสิทธิภาพ โดยชี้แจงจุดร่วมและภาระรับผิดชอบอย่างชัดเจน ▪ พัฒนากรอบยุทธศาสตร์ เพื่อส่งเสริมการทำงานร่วมกันและการตัดสินใจ

องค์ประกอบหลักของแผนการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

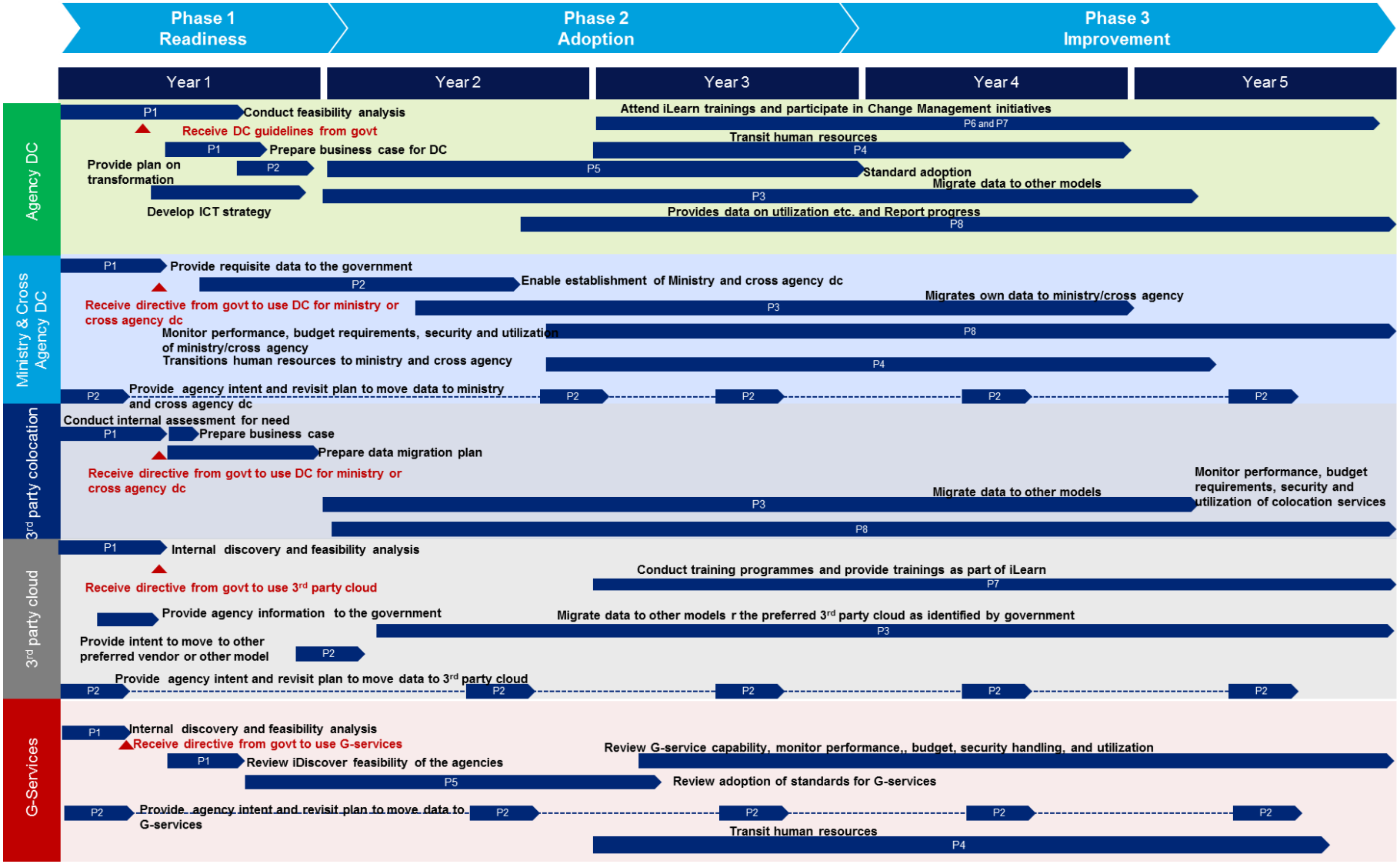
มิติที่เกี่ยวข้อง	องค์ประกอบหลักของแผนการดำเนินงาน
ความรับผิดชอบ	แผนการดำเนินงานฉบับนี้กำหนดให้ภาครัฐมีภาระรับผิดชอบในการจัดทำนโยบาย กรอบการดำเนินงาน การดำเนินโครงการ การริเริ่มต่างๆ การกำกับดูแลธรรมาภิบาล และการขับเคลื่อนยุทธศาสตร์เพื่อเพิ่มประสิทธิภาพด้านต้นทุน การฝึกอบรม และการบริหารจัดการข้อมูล นอกจากนี้ แผนการดำเนินงานฉบับนี้จัดทำขึ้นบนพื้นฐานภาระรับผิดชอบที่กำหนดให้หน่วยงานต่างๆ สามารถตัดสินใจเพื่อเลือกแนวทางที่เหมาะสมในอนาคต โดยหน่วยงานสามารถดำเนินการศึกษาความเป็นไปได้ การสร้างคุณประโยชน์ และการเปลี่ยนไปใช้ทางเลือกในรูปแบบอื่น
การจัดลำดับกิจกรรม	การจัดลำดับกิจกรรมในแผนการดำเนินงานนั้นเกิดจากการจัดลำดับความสำคัญของกิจกรรมที่สนับสนุนการเปลี่ยนแปลงและจะทำให้บรรลุผลในการขับเคลื่อนโครงการและสร้างคุณประโยชน์
หน่วยงานดำเนินงานได้ตามปกติ	แผนการดำเนินงานฉบับนี้ถูกจัดทำขึ้นเพื่อให้ความสามารถ (Capabilities) ที่อยู่ระหว่างการพัฒนาสามารถดำเนินการได้และส่งผลกระทบน้อยที่สุดต่อหน่วยงานเมื่อนำมาใช้งาน นอกจากนี้การย้ายข้อมูลจะดำเนินการในลักษณะที่หน่วยงานนั้นยังสามารถดำเนินงานได้ตามปกติ
ธรรมาภิบาลและยุทธศาสตร์	แผนการดำเนินงานฉบับนี้ถูกจัดทำขึ้นจากการกำหนดกรอบธรรมาภิบาลสำคัญและยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)
โครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ	แผนการดำเนินงานฉบับนี้ถูกจัดทำขึ้นบนพื้นฐานของการจัดตั้งโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศที่เหมาะสมและการระบุ 6 รูปแบบการดำเนินงานในอนาคตให้หน่วยงานได้เลือกใช้
การมีส่วนร่วม	แผนการดำเนินงานฉบับนี้มีการจัดตั้งคณะบริหารให้พร้อมก่อนการจัดตั้งคณะทำงานผลักดันการเปลี่ยนแปลงภายในหน่วยงาน ซึ่งคณะทำงานผลักดันการเปลี่ยนแปลงภายในหน่วยงานจะมีส่วนร่วมในการตัดสินใจและการเปลี่ยนแปลงในอนาคต
ข้อจำกัด	แผนการดำเนินงานฉบับนี้ไม่ครอบคลุมถึงข้อจำกัดด้านการจัดสรรงบประมาณและทรัพยากรที่อาจเกิดขึ้นหรือการควบรวมกับแผนงานและโครงการอื่นๆ
การดำเนินงาน	แผนการดำเนินงานฉบับนี้ประกอบด้วยหลายกิจกรรมหลักที่จำเป็นต้องปฏิบัติก่อนเริ่มต้นการดำเนินงานเพื่อเอื้อให้การดำเนินงานเป็นไปโดยสะดวก บรรเทาความเสี่ยง และจัดการการเปลี่ยนแปลง โดยการดำเนินงานในปีที่ 1 เป็นการเตรียมความพร้อมและทำการประเมินสถานะ เพื่อจุดประสงค์ดังกล่าว

แผนการดำเนินงานโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ฉบับย่อ

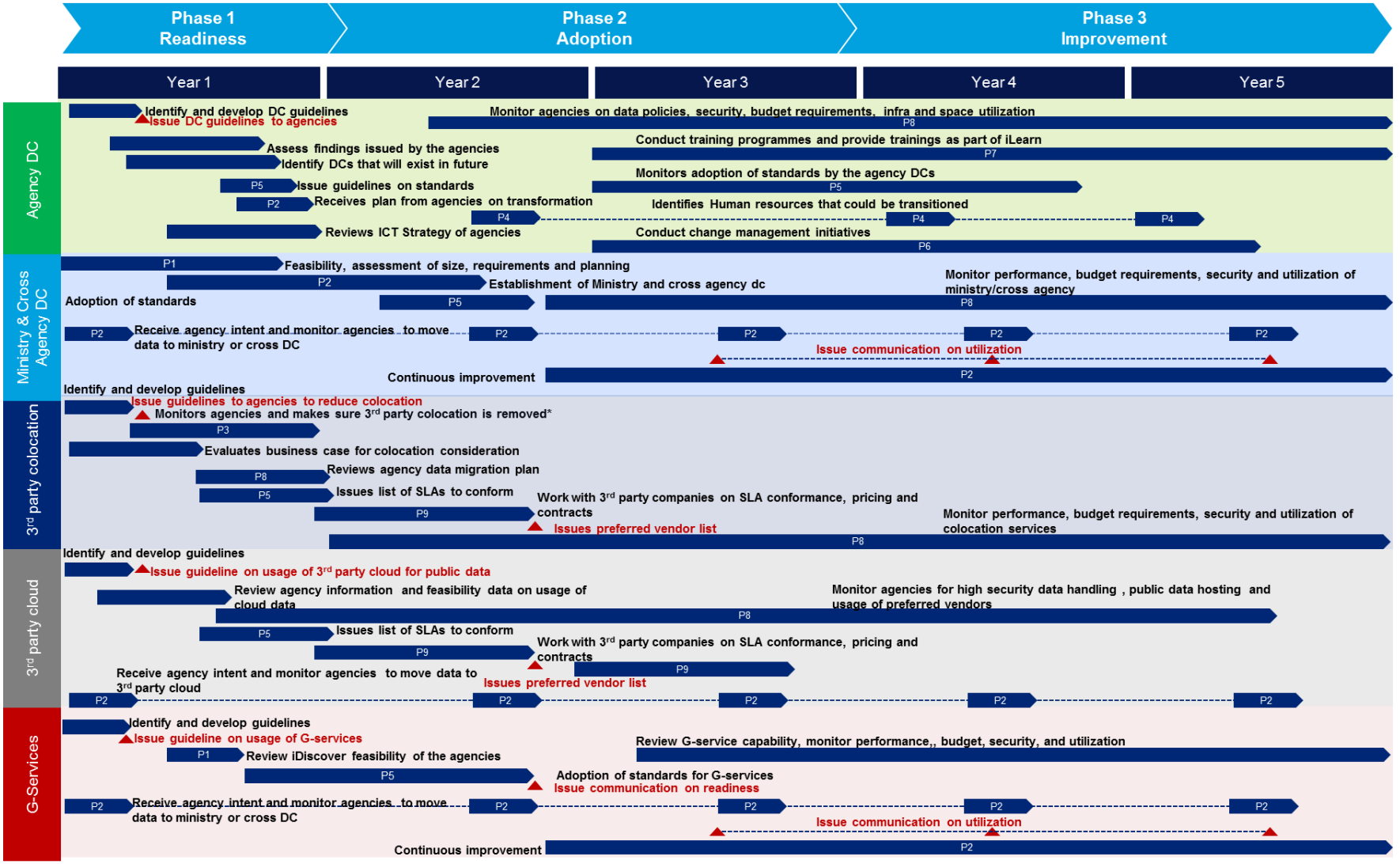
แผนการดำเนินงานโครงการพัฒนาศูนย์ข้อมูลภาครัฐฉบับย่อนี้ แสดงแผนงานและเป้าหมายสำคัญในระยะเวลา 5 ปีข้างหน้า



แผนการดำเนินงานโครงการโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) สำหรับหน่วยงานภาครัฐ



แผนการดำเนินงานโครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) สำหรับหน่วยงานกลาง (Central Administrative Office หรือ CAO)



โครงการเพื่อดำเนินงานยุทธศาสตร์โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ยุทธศาสตร์การดำเนินงานการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ประกอบด้วย 9 โครงการย่อย เพื่อขับเคลื่อนการบริหารจัดการและการดำเนินงานตามแผนการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) อย่างรวดเร็ว ดังต่อไปนี้

เลขที่โครงการ	ชื่อโครงการ และเป้าหมายโครงการ	คำอธิบายโครงการ
(P1) Project 1	 iDiscover *การศึกษาเชิงค้นคว้าเพื่อเข้าใจความเป็นไปได้ของรูปแบบและความต้องการทางเลือกด้านศูนย์ข้อมูล*	▪ โครงการนี้ครอบคลุมการศึกษาความเป็นไปได้ (Feasibility Study) และการวิเคราะห์โดยหน่วยงานเอง เพื่อระบุความต้องการที่แท้จริงและความพร้อมในการดำเนินงานของตน ▪ การศึกษาดังที่กล่าวมานี้ส่งผลให้หน่วยงานสามารถชี้แจงรายละเอียดการจำแนกประเภทข้อมูล การจัดการความปลอดภัยในปัจจุบัน ความพร้อมสำหรับรูปแบบการดำเนินงานในอนาคต แอปพลิเคชัน และรายละเอียดที่จำเป็น เป็นต้น ▪ ภาครัฐยังสามารถดำเนินการศึกษา iDiscover นี้เพื่อระบุความพร้อมและความเป็นไปได้ในการดำเนินงานศูนย์ข้อมูลระดับกระทรวง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน และการบริการโดยภาครัฐ ▪ โครงการ iDiscover จะส่งผลให้หน่วยงานต่างๆ สามารถระบุรูปแบบการดำเนินงานในอนาคตที่เหมาะสม เพื่อการดำเนินงานต่อไป
(P2) Project 2	 iTransform *โครงการปรับเปลี่ยนศูนย์ข้อมูลประจำหน่วยงานไปสู่ศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน*	▪ โครงการนี้ระบุหลักเกณฑ์สำหรับคัดเลือกศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน ▪ ขั้นตอนถัดไปคือการระบุข้อกำหนดสำคัญในการจัดตั้งศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน โดยข้อกำหนดครอบคลุมตั้งแต่มาตรฐาน ขนาดของศูนย์ข้อมูล โครงสร้างพื้นฐาน การรับประกันคุณภาพ และองค์ประกอบโครงสร้างพื้นฐานอื่นๆ ที่จำเป็น ▪ หลังจากทราบข้อกำหนดในการดำเนินงาน ศูนย์ข้อมูลเหล่านั้นจะได้รับการพัฒนาเป็นศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน ▪ ขั้นตอนถัดไปคือ การดำเนินแผนการสื่อสาร ติดตามความก้าวหน้าและอัตราการใช้งานศูนย์ข้อมูลที่ได้รับการพัฒนาแล้ว
(P3) Project 3	 iOptimize *โครงการย้ายข้อมูลจากศูนย์ข้อมูลรูปแบบหนึ่งไปสู่อีกรูปแบบหนึ่ง*	▪ โครงการนี้ส่งผลให้เกิดการเปลี่ยนถ่ายข้อมูลระหว่างศูนย์ข้อมูลรูปแบบต่างๆ หลังการศึกษาความเป็นไปได้และการวางแผนนั้นเสร็จสมบูรณ์ ▪ โครงการนี้ส่งผลให้เกิดการย้ายข้อมูลจากศูนย์ข้อมูลประจำหน่วยงานไปยังรูปแบบอื่นๆ เช่น การบริการโดยภาครัฐ ศูนย์ข้อมูลระดับกระทรวง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน และการบริการโดยหน่วยงานภายนอก ทั้งนี้โครงการนี้จะถ่ายโอนข้อมูลให้สอดคล้องกับระดับการรักษาความปลอดภัย ▪ โครงการนี้ยังนำไปสู่การบริหารจัดการศูนย์ข้อมูลแบบต่างๆ เช่น การลดจำนวนศูนย์ข้อมูล การเปลี่ยนแปลงการใช้บริการพื้นที่วางเครื่องแม่ข่าย (Colocation) ของหน่วยงานภายนอก เป็นต้น

เลขที่โครงการ	ชื่อโครงการ และเป้าหมายโครงการ	คำอธิบายโครงการ
(P4) Project 4	 iTransition *โครงการปรับใช้บุคลากรในหน่วยงาน*	▪ โครงการนี้มุ่งเน้นการปรับปรุงหน้าที่บุคลากรระหว่างรูปแบบการดำเนินงานในอนาคตต่างๆ ▪ หน้าที่ของบุคลากรจะมีการปรับปรุงให้สอดคล้องกับบทบาทหน้าที่สำหรับรูปแบบการดำเนินงานในอนาคตของหน่วยงาน
(P5) Project 5	 iAdopt *โครงการนำมาตรฐานที่กำหนดมาประยุกต์ใช้*	▪ โครงการนี้ส่งผลให้เกิดการนำมาตรฐานมาประยุกต์ใช้ในหน่วยงานต่างๆ รวมถึงการบริการโดยภาครัฐ (G-Services) ▪ โครงการนี้เริ่มต้นด้วยการวิเคราะห์ความเป็นไปได้ (Feasibility Analysis) ในการนำมาตรฐานมาใช้และระบุแนวทางการนำมาใช้สำหรับหน่วยงานต่างๆ ตาม “แผนการนำมาตรฐานมาใช้” ที่พัฒนาขึ้นมาในระยะที่ 1 ▪ หน่วยงานต่างๆ จะต้องประยุกต์ใช้มาตรฐานในช่วงระยะเวลา 5 ปีข้างหน้าตามแผนการนำมาตรฐานมาใช้ ▪ ภาครัฐจะติดตามสถานะความก้าวหน้าของการนำมาตรฐานมาประยุกต์ใช้ของหน่วยงานต่างๆ และการจัดทำรายงานสถานะ ▪ ภาครัฐจะต้องกำกับดูแลให้ศูนย์ข้อมูลระดับกระทรวง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน และการบริการโดยภาครัฐ ดำเนินงานสอดคล้องกับมาตรฐานที่กำหนดไว้
(P6) Project 6	 iChange *โครงการดำเนินกระบวนการและบริหารความเปลี่ยนแปลง*	▪ โครงการนี้เกี่ยวข้องกับกระบวนการบริหารความเปลี่ยนแปลง โดยเริ่มต้นจากการประเมินความพร้อมต่อการเปลี่ยนแปลง (Change Readiness Assessment) ภาครัฐจะทำการประเมินความพร้อมให้หน่วยงานต่างๆ ที่จะผ่านกระบวนการเปลี่ยนถ่าย เช่น การถ่ายโอนข้อมูล การยกเลิกศูนย์ข้อมูล การพัฒนาศูนย์ข้อมูลไปสู่ศูนย์ข้อมูลระดับกระทรวงหรือศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน และการปรับปรุงหน้าที่บุคลากร เป็นต้น ▪ ภาครัฐจะวางแผนการบริหารความเปลี่ยนแปลง วิเคราะห์ระดับการเปลี่ยนแปลงและระบุจุดบกพร่อง ▪ ภาครัฐจะกำหนดโครงการย่อยเพื่อแก้ไขจุดบกพร่อง และระบุเจ้าหน้าที่หรือตัวแทนการเปลี่ยนแปลง (Change Agent) ที่เอื้ออำนวยให้การเปลี่ยนแปลงสามารถทำได้ง่ายขึ้นกับหน่วยงานต่างๆ ▪ ภาครัฐจะติดตามสถานะการเปลี่ยนแปลง และจะใช้แผนการสื่อสาร วิธีการ และแผนการเปลี่ยนถ่าย เพื่อให้การเปลี่ยนแปลงเป็นไปอย่างราบรื่น

ประเภท	ชื่อโครงการและเป้าหมาย	คำอธิบายโครงการ
(P7) Project 7	 iLearn *โครงการฝึกอบรมทรัพยากรบุคคล*	▪ โครงการนี้จะระบุถึงความต้องการการฝึกอบรมสำหรับเจ้าหน้าที่ของหน่วยงาน ซึ่งการฝึกอบรมนับเป็นส่วนหนึ่งของแผนงานการเปลี่ยนแปลง ▪ การฝึกอบรมที่กล่าวมานี้จะครอบคลุมหลายมิติ เช่น การเปลี่ยนแปลงทางเทคโนโลยี ระบบคลาวด์ ประสิทธิภาพของศูนย์ข้อมูล การเพิ่มอัตราการใช้งาน มาตรฐาน ค่าประสิทธิภาพการใช้พลังงาน การจัดการการเปลี่ยนแปลง การบริหารจัดการโครงการ บทบาทหน้าที่และความรับผิดชอบ ประสิทธิภาพของผู้นำ การติดตามและรายงานผล และการดำเนินงานศูนย์ข้อมูลเฉพาะด้าน ▪ หน้าที่พัฒนาการฝึกอบรมเหล่านี้ สามารถจัดทำขึ้นได้โดยภาครัฐหรือหน่วยงานภายนอก ตามความเหมาะสม ▪ ภาครัฐจะจัดทำและแจกจ่ายตารางการฝึกอบรมเหล่านี้ ▪ ภาครัฐจะประเมินประสิทธิภาพการฝึกอบรมเหล่านี้
(P8) Project 8	 iMonitor *โครงการติดตามสถานะและรายงานความก้าวหน้า*	▪ โครงการนี้จะติดตามสถานะและความก้าวหน้าของการย้ายข้อมูลและการใช้รูปแบบการดำเนินงานในอนาคตทั้งหมด 6 รูปแบบ ▪ ภาครัฐจะทำการติดตามและรายงานผลความก้าวหน้าให้หน่วยงานต่างๆ ทราบและสนับสนุนการดำเนินงาน
(P9) Project 9	 iNegotiate *โครงการเจรจาอัตราค่าใช้จ่าย, การบริการ, และ SLA กับหน่วยงานผู้ให้บริการภายนอก*	▪ โครงการนี้มีระยะเวลาที่สั้น ซึ่งภาครัฐจะเจรจาอัตราค่าใช้จ่าย ข้อกำหนดระดับการให้บริการ (SLA) ข้อกำหนดด้านทรัพยากรบุคคล การให้บริการ และคุณภาพกับผู้ให้บริการภายนอกที่ให้บริการพื้นที่วางเครื่องแม่ข่ายและบริการคลาวด์สำหรับหน่วยงานภาครัฐทั้งหมด

สมมติฐานในการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

สมมติฐาน	คำอธิบาย
ภาระรับผิดชอบ	แผนฉบับนี้ใช้นิยามภาระรับผิดชอบตามที่ระบุในหลักการการกำหนดแนวทางดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) โดยในการดำเนินงานระยะที่ 1 จะมีการจัดทำภาระรับผิดชอบในรายละเอียด
ความพร้อมในระยะที่ 1	แผนฉบับนี้ตั้งสมมติฐานว่าการเริ่มทำกิจกรรมการเตรียมการ (Pre-Implementation Activities) มาก่อนการดำเนินงานระยะที่ 2 ซึ่งถือได้ว่ากิจกรรมการเตรียมการนั้นเป็นส่วนหนึ่งของการดำเนินงานระยะที่ 1
การจัดสรรทรัพยากร	แผนฉบับนี้ตั้งสมมติฐานว่าจะมีการจัดเตรียมทรัพยากรทั้งทางด้านบุคลากรโครงการและข้อมูลจากหน่วยงานต่างๆ ในระดับที่เหมาะสมเพื่อให้เกิดการเปลี่ยนแปลง การดำเนินงานระยะที่ 1 เป็นการรวบรวมผลการศึกษาและการวิเคราะห์ต่างๆ เพื่อระบุการเปลี่ยนแปลง
การบริหารความเปลี่ยนแปลง	แผนฉบับนี้ตั้งสมมติฐานว่าควรมีการดำเนินกิจกรรมเพื่อเตรียมพร้อมต่อการเปลี่ยนแปลง เพื่อให้การเปลี่ยนแปลงนั้นประสบผลสำเร็จ
ผู้มีส่วนได้เสีย	แผนฉบับนี้ตั้งสมมติฐานว่าผู้มีส่วนได้เสียภายนอกจะไม่กีดขวางหรือทำให้การดำเนินงานล่าช้า (เช่น หน่วยงานต่างๆ และสถานการณ์ทางการเมือง)
กระบวนการและนโยบาย	แผนฉบับนี้ตั้งสมมติฐานว่าจะมีการกำหนดกระบวนการและนโยบายให้สอดคล้องกับภาระรับผิดชอบต่อการขับเคลื่อนการเปลี่ยนแปลงในระยะที่ 1
ยุทธศาสตร์	แผนนี้ตั้งสมมติฐานว่าการดำเนินงานจะไม่ปรับเปลี่ยนโครงสร้างองค์กรหรือแผนการดำเนินงานนี้อย่างมีนัยสำคัญ
ความต้องการทรัพยากร	แผนนี้ตั้งสมมติฐานว่าจะมีการกำหนดความต้องการทรัพยากรที่จำเป็นต่อการดำเนินงานและธรรมาภิบาลไว้ให้พร้อมและสามารถใช้งานได้อย่างราบรื่น

ปัจจัยความสำเร็จในการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ปัจจัยความสำเร็จ	ข้อกำหนด
การสนับสนุนและความมุ่งมั่นจากภาครัฐ	■ ภาครัฐมีส่วนร่วมอย่างต่อเนื่อง รวมถึง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานด้านเทคโนโลยีอื่นๆ ให้การสนับสนุนและขับเคลื่อนโครงการ
ความพร้อมของทรัพยากรบุคคล	■ จัดสรรทรัพยากรบุคคลที่เหมาะสมสำหรับการกำกับดูแลธรรมาภิบาล ■ กำหนดแผนสำรอง เพื่อรองรับความพร้อมของทรัพยากรบุคคล ■ จัดการฝึกอบรมและการเรียนรู้ให้แก่บุคลากรอย่างต่อเนื่อง เพื่อสนับสนุนการเปลี่ยนแปลงและเพิ่มประสิทธิภาพอย่างรวดเร็ว
กรอบยุทธศาสตร์	■ กำหนดยุทธศาสตร์และกรอบการทำงานอย่างชัดเจน
การจัดสรรทรัพยากรและการวางแผนทางการเงิน	■ การยอมรับ GDCM เสมือนวาระสำคัญของภาครัฐ ■ ระบุทรัพยากรทางการเงินและจัดเตรียมงบประมาณสำหรับการจัดตั้งศูนย์ข้อมูลระดับกระทรวง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน การศึกษาความเป็นไปได้โดยภาครัฐและหน่วยงาน รวมทั้งการพัฒนาการบริการโดยภาครัฐ และการนำมาตรฐานมาใช้งาน
ความมุ่งมั่นจากทุกภาคี	■ ความมุ่งมั่นจากทุกภาคี ได้แก่ ภาครัฐ หน่วยงานตัวแทนภาครัฐในการบริหารความเปลี่ยนแปลง พันธมิตรด้านเทคโนโลยี หน่วยงานและกระทรวงต่างๆ รวมถึงภาคเอกชน ■ มีการประสานงานอย่างแข็งขันระหว่างผู้มีส่วนได้ส่วนเสียสำคัญ เพื่อพัฒนาและดำเนินงานยุทธศาสตร์ GDCM
โครงสร้างพื้นฐานมีความยั่งยืน	■ จัดเตรียมโครงสร้างพื้นฐานให้พร้อมใช้งานตามที่กำหนดในยุทธศาสตร์ GDCM ■ จัดเตรียมความปลอดภัยเครือข่ายและข้อมูลให้เป็นไปตามแผนที่วางไว้ ■ จัดหาโครงสร้างพื้นฐาน เพื่อรองรับการเปลี่ยนแปลง
ความพร้อมใช้งานของงานวิจัยและผลการศึกษา	■ ดำเนินการศึกษาต่างๆ เพื่อกำหนดและขยายรายละเอียดยุทธศาสตร์สำหรับการดำเนินงานในระยะที่ 1 ■ ระบุตัวแทนการเปลี่ยนแปลง (Change Agent) ■ ระบุหน่วยงานนำร่อง

ความเสี่ยงในการดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ความเสี่ยง	แนวทางบรรเทาความเสี่ยง
การเปลี่ยนแปลงอาจกระทบประสิทธิภาพการทำงาน	▪ จัดเตรียมโครงสร้างการเปลี่ยนแปลงให้พร้อม เพื่อช่วยจัดการกระบวนการเปลี่ยนถ่าย ▪ ระบุจุดที่มีปัญหาหลักและเฝ้าติดตามอย่างใกล้ชิด ▪ จัดสรรเวลาในการเสริมสร้างความสามารถใหม่ๆ อย่างเพียงพอ
การสูญเสียทรัพยากรบุคคลไปกับการเปลี่ยนแปลง	▪ กำหนดนโยบายรักษาบุคลากร เพื่อสร้างแรงกระตุ้นแก่บุคลากรหลัก ▪ เปิดโอกาสให้บุคลากรหลักมีส่วนร่วมในกระบวนการเปลี่ยนแปลง ▪ พูดถึงโอกาสในเส้นทางอาชีพ (Career Path) กับผู้มีโอกาสได้รับผลกระทบอย่างเปิดเผย ▪ ฝึกอบรมข้ามสายงานทุกส่วนที่เป็นไปได้ ▪ ดำเนินการแบ่งปันองค์ความรู้อย่างเป็นระบบ
ไม่อาจหาบุคลากรที่เหมาะสำหรับบทบาทหน้าที่สำคัญ	▪ จัดสรรเวลาอย่างเพียงพอในการสรรหา และคัดเลือกบุคลากรใหม่ ▪ พิจารณาบนพื้นฐานความเป็นจริงถึงตัวเลือกที่มีและเปิดกว้างต่อการปรับเปลี่ยนขอบเขตหน้าที่ เพื่อรองรับบุคลาการที่มีความสามารถ ▪ จัดทำแผนพัฒนาอาชีพสำหรับบุคลากรภายในที่มีความสามารถ
ไม่สามารถคงระดับคุณภาพในการดำเนินงาน	▪ ระบุข้อมูลที่จำเป็นต้องเก็บรักษาไว้อย่างชัดเจน ตลอดจนระบุข้อมูลและแอปพลิเคชันที่ต้องปรับเปลี่ยน ▪ เฝ้าติดตามประเด็นเหล่านี้ ระหว่างการดำเนินงาน
ขาดเทคโนโลยีที่เหมาะสม เพื่อสนับสนุนกระบวนการเปลี่ยนแปลง	▪ กำหนดความต้องการทางเทคโนโลยี เพื่อรองรับการเปลี่ยนแปลงเชิงองค์กร ▪ วางแผนขับเคลื่อนการเปลี่ยนแปลงองค์กร เพื่อรองรับการดำเนินงานด้านเทคโนโลยี หรือเร่งการดำเนินงานด้านเทคโนโลยี เพื่อรองรับการการเปลี่ยนแปลงองค์กร ▪ กำหนดรูปแบบทางเลือกที่มีความพร้อม เช่น 3rd Party Cloud เพื่อรองรับกระบวนการเปลี่ยนแปลง
เกิดแรงต่อต้านต่อการเปลี่ยนแปลงและหน่วยงานไม่ยอมรับวิธีการทำงานที่ตั้งเป้าหมายไว้	▪ ระบุข้อกำหนดของหน่วยงานที่จำเป็นต่อการสนับสนุนการเปลี่ยนแปลงในระยะที่ 1 ▪ พิจารณาเริ่มแผนจัดการการเปลี่ยนแปลงที่ตอบโจทย์ด้านการรับรู้ ความสามารถ กลไกสนับสนุน และ ตัวอย่าง เพื่อสนับสนุนวิธีการทำงานแบบใหม่
ความเปลี่ยนแปลงกระทบความสัมพันธ์ต่างๆ ของหน่วยงาน	▪ ใช้แผนสื่อสารชี้แจงกับหน่วยงานต่างๆ ให้เกิดความเข้าใจ ▪ จัดเตรียมคำแนะนำให้หน่วยงานกลาง (Central Administrative Office) ถึงแนวทางทำงานร่วมกับหน่วยงานต่างๆ ระหว่างกระบวนการเปลี่ยนแปลง
โครงสร้างธรรมาภิบาลและโครงสร้างพื้นฐานไม่สามารถรองรับการเปลี่ยนแปลงได้	▪ ดำเนินการศึกษาความเป็นไปได้ เพื่อเตรียมความพร้อมการดำเนินงานในระยะที่ 1 ▪ จัดทำแผนดำเนินงานให้สอดคล้องกับการเปลี่ยนแปลงอื่นๆ ที่กำลังดำเนินอยู่ ▪ เฝ้าติดตามความพร้อมต่อการเปลี่ยนแปลงและการมีส่วนร่วมของบุคลากรตลอดกระบวนการเปลี่ยนแปลง

ความเสี่ยง	แนวทางบรรเทาความเสี่ยง
เทคโนโลยีไม่รองรับการดำเนินงาน	■ ใช้แผนความต่อเนื่องในการดำเนินงาน (Business Continuity Plan หรือ BCP) สำหรับการดำเนินงานของหน่วยงาน โดยหน่วยงานส่วนใหญ่จัดทำ BCP ขึ้นสำหรับช่วงการเปลี่ยนถ่าย ■ ใช้แผนกู้คืนภัยพิบัติ (Disaster Recovery Plan)
ปัญหาด้านความเป็นส่วนตัวและความปลอดภัย	■ ดำเนินมาตรการความมั่นคงปลอดภัยที่กล่าวถึงในการนำมาตรฐานมาใช้ ■ เตรียมความพร้อมการดำเนินงานด้านการจัดการความปลอดภัยตามที่ระบุไว้ในระยะที่ 1

19. แนวทางปฏิบัติด้านยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ในอดีตที่ผ่านมา หน่วยงานภาครัฐของไทยมุ่งเน้นการลงทุนเพื่อพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศในการรองรับความต้องการศูนย์ข้อมูลที่เพิ่มขึ้นเท่านั้น แต่เนื่องด้วยปัจจัยที่สำคัญต่อการขับเคลื่อนการดำเนินงานและข้อจำกัดต่างๆ ที่มีในปัจจุบันนั้น หน่วยงานภาครัฐของไทยจำเป็นต้องให้ความสำคัญกับองค์ประกอบที่สำคัญอื่นๆ เช่น ประสิทธิภาพของศูนย์ข้อมูล การลดความซับซ้อนของโครงสร้างพื้นฐาน การรักษาความปลอดภัย ประสิทธิภาพด้านต้นทุนโดยรวม และประสิทธิภาพของการใช้พลังงาน เพื่อส่งเสริมการเติบโตอย่างยั่งยืน

ยุทธศาสตร์ขับเคลื่อนการเปลี่ยนแปลงของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) จะใช้ประโยชน์จากแนวทางและกฎระเบียบกับการบริหารความเปลี่ยนแปลง การนำโยบายที่สำคัญมาประยุกต์ใช้ การสั่งการ และแผนงานที่จัดทำไว้ควบคู่กับการดำเนินงานของหน่วยงานต่างๆ

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐนี้จะก่อให้เกิดคุณประโยชน์สำคัญของโครงสร้างพื้นฐานด้านข้อมูลที่มีประสิทธิภาพ ดังนั้น โครงสร้างพื้นฐานด้านข้อมูลรูปแบบใหม่ เช่น การบริการโดยภาครัฐ (G-Services) การบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) การบริการร่วมกันในรูปแบบของศูนย์ข้อมูลระดับกระทรวง (Ministry-Level Data Center) และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน (Cross-Agency Data Center) จะสามารถผลักดันการเติบโตอย่างมหาศาลในด้านการพัฒนาศักยภาพ ความสามารถในการรองรับปริมาณข้อมูลขนาดใหญ่ การเตรียมความพร้อมรองรับอนาคต และความยั่งยืนในระยะยาวอีกด้วย

การวัดประสิทธิภาพของยุทธศาสตร์นี้จะดำเนินการในช่วงระยะเวลา 2-3 ปีข้างหน้า โดยอาศัยตัวชี้วัดที่จะได้รับการปรับให้เหมาะสมยิ่งขึ้นในปีที่ 1 ดังต่อไปนี้

1. การใช้ประโยชน์ทรัพย์สิน พื้นที่จัดเก็บข้อมูล และทรัพยากรอย่างมีประสิทธิภาพ (Effective Utilization of Assets, Capacity and Resources)
2. การบริการร่วมกัน (Shared Services)
3. ประสิทธิภาพด้านต้นทุน (Cost Efficiency)
4. การยกระดับความปลอดภัย (Enhanced Security)
5. กรอบยุทธศาสตร์ (Strategic Framework)

1. การใช้ประโยชน์ทรัพย์สิน พื้นที่จัดเก็บข้อมูล และทรัพยากรอย่างมีประสิทธิภาพ

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐนี้เสนอแนวทางการใช้ประโยชน์จากองค์ประกอบต่างๆ อย่างมีประสิทธิภาพ เช่น ทรัพย์สิน (ทรัพย์สินภาครัฐในรูปแบบของศูนย์ข้อมูล เครือข่าย ปัจจัยสำคัญต่างๆ ต่อการจัดตั้งศูนย์ข้อมูล และ การบริการโดยภาครัฐ) พื้นที่และความสามารถในการจัดเก็บข้อมูล (ในรูปแบบของพื้นที่ศูนย์ข้อมูล แบนด์วิธ เครื่องแม่ข่าย และอุปกรณ์จัดเก็บข้อมูล) และทรัพยากรต่างๆ (รวมถึง ทรัพยากรบุคคล) โดยหน่วยงานสามารถใช้ทรัพยากรต่างๆ ที่มีเพื่อรองรับความต้องการของตนเอง (รวมถึงมีความสามารถในการรองรับการขยายตัวของบริการ เพื่อรองรับความต้องการที่เพิ่มขึ้น) โดยเกิดความสิ้นเปลืองน้อยที่สุด รูปแบบของโครงสร้างพื้นฐานด้านข้อมูลในอนาคตถูกจัดทำขึ้น โดยคำนึงถึงความสามารถในการรองรับการขยายตัวของบริการและความจำเป็นที่

จะต้องเพิ่มอัตราการใช้งานทรัพย์สินภาครัฐ การให้ความสำคัญในการใช้ประโยชน์จากพื้นที่จัดเก็บข้อมูลและทรัพย์สิน ส่งผลให้ภาครัฐสามารถสนับสนุนการดำเนินงานของหน่วยงานและประเทศได้อย่างคล่องตัว

2. การบริการร่วมกัน

หนึ่งในองค์ประกอบสำคัญของยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) ภายใต้กรอบการพัฒนาเศรษฐกิจดิจิทัลและการดำเนินงานโดยยึดประชาชนเป็นศูนย์กลาง คือ ความสามารถในการให้บริการร่วมกัน (Shared Services) และยุทธศาสตร์ที่จะขยายบริการดังกล่าว การบริการร่วมกันสามารถพิจารณาได้ในหลายมิติ เช่น การยกระดับความพร้อมใช้งาน เสถียรภาพ ความปลอดภัย ประสิทธิภาพด้านต้นทุน การตอบสนองต่อความต้องการของประชาชน และการปฏิบัติตามมาตรฐาน นอกจากนี้ ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐยังเน้นย้ำการใช้รูปแบบการบริการร่วมกันที่หลากหลาย เช่น การเพิ่มความสามารถของหน่วยงานในการให้บริการร่วมกันแก่หน่วยงานใกล้เคียงเพื่อเพิ่มอัตราการใช้งานทรัพยากรของตนเอง รวมถึงการใช้ประโยชน์จากศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงานที่พัฒนาขึ้น เป็นต้น การบริการร่วมกันยังรวมถึงการใช้ประโยชน์จากการบริการโดยภาครัฐ (G-Services) ซึ่งครอบคลุม G-Cloud และการให้บริการพื้นที่วางเครื่องแม่ข่ายของภาครัฐ นอกจากนี้ หน่วยงานอาจเลือกใช้การบริการโดยหน่วยงานภายนอก เช่น 3rd Party Cloud เพื่อจัดเก็บข้อมูลได้เช่นกัน ที่สำคัญ การทราบถึงจำนวนหน่วยงานและระดับการเปลี่ยนแปลงที่ภาครัฐมีการใช้บริการร่วมกันเป็นประเด็นสำคัญในการประเมินตัวชี้วัดความสำเร็จ (KPI) นี้

3. ประสิทธิภาพด้านต้นทุน

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) นี้แสดงให้เห็นถึงประสิทธิภาพด้านต้นทุนที่ดีกว่าในอดีต ภาครัฐควรลดการพึ่งพาการลงทุนด้านโครงสร้างพื้นฐานโดยอาศัยเทคโนโลยีทันสมัยในรูปแบบของการบริการร่วมกันเพื่อประสิทธิภาพด้านต้นทุนที่สูงสุด ทั้งนี้ ประสิทธิภาพของการบริการร่วมกันในรูปแบบของศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงานเป็นการส่งเสริมโครงสร้างพื้นฐานแบบบูรณาการเพื่อรองรับการใช้งานของกระทรวงและหน่วยงานต่างๆ พร้อมๆ กัน รูปแบบการบริการร่วมกันที่กล่าวมานี้ส่งผลให้เกิดทางเลือกที่ปลอดภัย บูรณาการ คุ้มค่า และยืดหยุ่นแก่หน่วยงานต่างๆ ในการให้บริการอย่างราบรื่น นอกจากนี้ หน่วยงานต่างๆ ได้พิจารณาทางเลือกการให้บริการในรูปแบบอื่น ได้แก่ การบริการโดยภาครัฐ (G-Services) และการบริการโดยหน่วยงานภายนอก (3rd Party Services: IaaS, PaaS และ SaaS) ด้วยเช่นกัน โดยยุทธศาสตร์ใหม่ในการพัฒนาศูนย์ข้อมูลนี้จะช่วยให้หน่วยงานต่างๆ สามารถมุ่งเน้นการปฏิบัติหน้าที่ตามภารกิจหลัก จึงเป็นการช่วยลดปัญหาด้านทรัพยากรบุคคลและปัญหาด้านเจ้าหน้าที่ดูแลศูนย์ข้อมูลที่ไม่เพียงพอโดยอาศัยบริการคลาวด์ นอกจากนี้ การบริการโดยภาครัฐ (G-Services) เป็นโครงสร้างพื้นฐานที่มีความยืดหยุ่นสูงและอยู่ในความดูแลของภาครัฐ ดังนั้นการบริการโดยภาครัฐจะสามารถให้บริการคลาวด์แก่หน่วยงานต่างๆ ได้อย่างปลอดภัย ด้วยเหตุนี้ ภาครัฐจะต้องจัดทำและรักษาข้อตกลงระดับการให้บริการ (SLA) การรักษาความปลอดภัย และแนวทางปฏิบัติด้านมาตรฐานสำหรับการบริการโดยภาครัฐ (G-Services) นี้ ที่สำคัญ หากพิจารณาทางด้านการเงินแล้ว เป้าหมายที่สำคัญที่สุดของภาครัฐคือการบริหารจัดการการใช้จ่ายงบประมาณในการดำเนินงานอย่างมีประสิทธิภาพและได้รับผลตอบแทนจากการลงทุนสูงสุด

4. การยกระดับความปลอดภัย

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) พิจารณาการรักษาความปลอดภัยเสมือนหนึ่งในปัจจัยสำคัญที่สุดสำหรับการพัฒนาศูนย์ข้อมูล ดังนั้น จึงเป็นสิ่งสำคัญที่ภาครัฐต้องให้การรักษาและจัดการความปลอดภัยข้อมูลของประเทศ ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐเล็งเห็นความสำคัญที่ต้องปกป้องข้อมูล เนื่องจากข้อมูลภาครัฐเปรียบเสมือนทรัพย์สินของประเทศ

ภายใต้ยุทธศาสตร์นี้ ภาครัฐส่งเสริมให้หน่วยงานต่างๆ เลือกใช้งานรูปแบบการดำเนินงานในอนาคตทั้ง 6 รูปแบบอย่างรอบคอบเพื่อยกระดับการรักษาความปลอดภัยของข้อมูล ซึ่งในขั้นตอนต่อไป ภาครัฐจะดำเนินการศึกษาต่างๆ เพื่อกำหนดสถานะความปลอดภัยของหน่วยงานที่จะมีการประเมินในระยะต่างๆ ของการดำเนินงานการเปลี่ยนแปลง ทั้งนี้ การจัดการข้อมูลของประเทศอย่างเหมาะสมจะช่วยยกระดับความสามารถในการจัดการความปลอดภัยและกลไกการจัดการข้อมูลในอนาคตต่อไปเป็นเวลาหลายปี

5. กรอบยุทธศาสตร์

ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) กำหนดเหตุผลเชิงยุทธศาสตร์ จุดมุ่งหมาย หน้าที่ และความคิดริเริ่มสำคัญที่ภาครัฐวางแผนจะดำเนินงานยุทธศาสตร์การพัฒนาศูนย์ข้อมูล ตัวชี้วัดความสำเร็จที่สำคัญยิ่งของยุทธศาสตร์นี้คือ ความมีประสิทธิภาพของการกำหนดยุทธศาสตร์ สัตยาบัน การบังคับใช้ และการดำเนินงาน ตัวชี้วัดความสำเร็จ (KPI) สามารถกำหนดขึ้นได้ทั้งในระดับภาครัฐและหน่วยงานเพื่อสนับสนุนการดำเนินงานยุทธศาสตร์อย่างมีประสิทธิภาพ

ตารางด้านล่างนี้แสดงถึงตัวชี้วัดความสำเร็จ (KPI) ที่สามารถนำไปใช้ในการประเมินประสิทธิภาพการดำเนินงานตามยุทธศาสตร์

มิติ	ตัวชี้วัดความสำเร็จ (KPIs)
การใช้งานทรัพย์สินและพื้นที่จัดเก็บข้อมูล	• % ของศูนย์ข้อมูลที่ยกเลิกการให้บริการ • % ของความต้องการศูนย์ข้อมูลที่ลดลง • % การใช้งานพื้นที่จัดเก็บข้อมูลของศูนย์ข้อมูลเพิ่มขึ้น • % การใช้งานเครื่องแม่ข่ายเพิ่มขึ้น
การใช้งานทรัพยากรบุคคล	• % ของทรัพยากรบุคคลที่ได้รับการฝึกอบรมด้านกระบวนการทำงานของศูนย์ข้อมูล • % ของทรัพยากรบุคคลที่มีการใช้งานร่วมกันและถ่ายโอน • จำนวนครั้งการจัดฝึกอบรม • % ของเจ้าหน้าที่ IT อาวุโสที่ได้รับการฝึกอบรมด้านกระบวนการทำงานของหน่วยงานและความเชื่อมโยงกับศูนย์ข้อมูล • % ของเจ้าหน้าที่ IT ที่ได้รับการฝึกอบรมความเชี่ยวชาญด้านศูนย์ข้อมูล
การบริการร่วมกัน	• จำนวนศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงานถูกจัดตั้งขึ้น • จำนวนหน่วยงานที่ทำการย้ายข้อมูล • % ของข้อมูลที่จัดเก็บไว้ในศูนย์ข้อมูลระดับกระทรวง/ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน 3rd Party Cloud และ G-Services

มิติ	ตัวชี้วัดความสำเร็จ (KPIs)
	• จำนวนผู้ให้บริการภายนอก พร้อมอัตราค่าใช้จ่ายที่มีการต่อรอง และบัญชีรายชื่อผู้ให้บริการที่ภาครัฐจัดเตรียมไว้ • % ของการบริการที่ดำเนินการอย่างอิสระ โดยใช้ G-Services • % ของการบริการที่ดำเนินการอย่างอิสระ โดยใช้ศูนย์ข้อมูลระดับกระทรวงและศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน • % ของการบริการที่ดำเนินการอย่างอิสระ โดยใช้ 3rd Party Cloud
การเพิ่มประสิทธิภาพด้านต้นทุน	• % ของการเพิ่ม/ลดงบประมาณการลงทุน เนื่องจากการเพิ่มประสิทธิภาพ • % ของการเพิ่ม/ลดต้นทุนการดำเนินงาน เนื่องจากการเพิ่มประสิทธิภาพ • % การลดลงทั้งหมดในการจัดสรรงบประมาณ
ความปลอดภัย	• % ของศูนย์ข้อมูลที่ย้ายข้อมูลตามแผน
กรอบยุทธศาสตร์	• โครงสร้างองค์กรในการขับเคลื่อนยุทธศาสตร์ GDCM • นโยบายและกรอบการทำงานของภาครัฐ • หน่วยงานต่างๆ ส่งรายงานวิเคราะห์ศึกษาความเป็นไปได้ • ยุทธศาสตร์ ICT ของกระทรวงและหน่วยงานต่างๆ • แผนการดำเนินงาน ICT ของกระทรวงและหน่วยงานต่างๆ

20. แนวทางปฏิบัติด้านทรัพยากรบุคคลของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ทรัพยากรบุคคลมีความสำคัญต่อโครงสร้างพื้นฐานภาครัฐ ในปัจจุบันศูนย์ข้อมูลมีบทบาทสำคัญในการพัฒนาและการปฏิบัติงานในทุกภาคส่วนของเศรษฐกิจ ยิ่งโครงสร้างพื้นฐานด้านข้อมูลมีความซับซ้อนมากขึ้น การสรรหาบุคลากรที่เหมาะสมและในปริมาณที่เพียงพอกลายเป็นความท้าทายสำคัญ นอกจากนี้ อุตสาหกรรมศูนย์ข้อมูลกำลังเผชิญปัญหาการขาดแคลนบุคลากร ซึ่งสวนทางกับความต้องการบุคลากรด้านศูนย์ข้อมูลที่มีเพิ่มมากขึ้น

ปัจจัยที่ขับเคลื่อนอุตสาหกรรมศูนย์ข้อมูลนั้นมีความคล้ายคลึงกับปัจจัยที่ผลักดันให้เกิดการเติบโตของอินเทอร์เน็ต อินเทอร์เน็ตบรอดแบนด์ ระบบคลาวด์ การพาณิชย์อิเล็กทรอนิกส์ เว็บแอปพลิเคชัน โซเชียลเน็ตเวิร์ค การส่งไฟล์วิดีโอ รวมไปถึงการเล่นเกม เหล่านี้ล้วนส่งผลให้อินเทอร์เน็ตเป็นปัจจัยสำคัญในต่อภาคธุรกิจ ผู้บริโภค และความต้องการขยายตัวของศูนย์ข้อมูล ดังนั้น ความต้องการบุคลากรที่มีคุณสมบัติเหมาะสมจึงเพิ่มขึ้นเพื่อรองรับการขยายตัวอย่างรวดเร็วนั้น หน่วยงานภาครัฐของประเทศไทยเชื่อว่าความสามารถของทรัพยากรบุคคลเป็นหนึ่งในอุปสรรคสำคัญที่สุดที่ศูนย์ข้อมูลกำลังประสบอยู่ทุกวันนี้

ตารางด้านล่างนี้ระบุกรอบหน้าที่และความเชี่ยวชาญในระดับต่างๆ ของบุคลากรที่ศูนย์ข้อมูลต้องการ กรอบหน้าที่และความเชี่ยวชาญเหล่านี้สอดคล้องกับรูปแบบการดำเนินงานในอนาคตทั้งหมด ทั้งกรณี ศูนย์ข้อมูลของภาครัฐและผู้ให้บริการศูนย์ข้อมูลภายนอก

วิศวกรทดสอบศูนย์ข้อมูล (Data Center Test Engineer)	ผู้ได้รับมอบหมายให้จัดเตรียมสภาพแวดล้อม เพื่อทดสอบอุปกรณ์คอมพิวเตอร์และเครือข่ายภายในศูนย์ข้อมูล พร้อมทั้งระบุประเด็นปัญหาและสาเหตุสำคัญ
เจ้าหน้าที่เทคนิคด้านสภาพแวดล้อมและความปลอดภัยศูนย์ข้อมูล (Data Center Environmental and Safety Technician)	ให้การช่วยเหลือและคอยติดตามกิจกรรมต่างๆ ในด้านสภาพแวดล้อม ความสมบูรณ์ และความปลอดภัยภายในศูนย์ข้อมูล โดยมีหน้าที่ตรวจสอบปัญหาด้านความปลอดภัย รวมทั้งดำเนินการฝึกอบรมด้านสิ่งแวดล้อม
สถาปนิกด้านโครงสร้างพื้นฐาน (Infrastructure Architect)	เป็นผู้ออกแบบศูนย์ข้อมูล ดูแลการบริการสนับสนุนทั้งหมด เช่น ระบบทำความเย็นและไฟฟ้า
ผู้จัดการศูนย์ข้อมูล (Data Center Manager)	มีหน้าที่ดูแลการดำเนินงานศูนย์ข้อมูลในภาพรวม ผู้จัดการศูนย์ข้อมูลจึงต้องมีความรู้หลากหลายที่เกี่ยวข้องกับศูนย์ข้อมูลทั้งหมด ตั้งแต่ความเข้าใจเกี่ยวกับเครือข่ายและระบบปฏิบัติการ จนถึงแนวทางและนโยบาย เพื่อทราบระเบียบการและกระบวนการที่ถูกต้อง
วิศวกรไฟฟ้า (Electrical Engineer)	ร่วมกันทำงานในรูปแบบคณะทำงาน มีหน้าที่แก้ปัญหาต่างๆ ในศูนย์ข้อมูล ในเรื่องระบบไฟฟ้า ระบบพลังงานของศูนย์ข้อมูล การติดตั้งเครื่องแม่ข่าย การเดินสายสัญญาณ และการวางแผนพื้นที่ใช้งานของศูนย์ข้อมูล

นักวางแผนการบำรุงรักษาศูนย์ข้อมูล (Data Center Maintenance Planner/Scheduler)	มีหน้าที่สื่อสารภายในและทำการติดต่อกับผู้ใช้บริการอย่างสม่ำเสมอ เพื่อวางแผนจากการวิเคราะห์ความต้องการของผู้ใช้บริการและจัดการโครงการตลอดระยะเวลาการดำเนินงานของโครงการ รวมทั้งสนับสนุนการวางแผนและกำหนดตารางดำเนินกระบวนการต่างๆ อย่างมีประสิทธิภาพ นอกจากนี้ จำเป็นต้องมีความรู้เกี่ยวกับอุปกรณ์และความเชี่ยวชาญทางเทคนิคในการพัฒนาการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)
เจ้าหน้าที่วิศวกรด้านระบบควบคุมศูนย์ข้อมูล (Data Center Control Systems Staff Engineer)	เจ้าหน้าที่ในตำแหน่งนี้ต้องมีประสบการณ์ไม่น้อยกว่า 10 ปี รวมทั้งมีปริญญาที่เกี่ยวข้อง พร้อมทั้งมีประสบการณ์ในด้านโครงสร้างพื้นฐานสำคัญ เช่น ระบบอัตโนมัติอุตสาหกรรม (Industrial Automation), SCADA Systems, และ PLC รวมทั้งสามารถให้การช่วยเหลือทางเทคนิคแก่คณะวิศวกรและคณะปฏิบัติงาน หน้าที่นี้ยังครอบคลุมไปถึงการแก้ไขปัญหาระบบควบคุมไฟฟ้าหลัก เช่นเดียวกับการจัดซื้อและจัดการประเด็นปัญหาที่เกิดจากผู้ให้บริการ
วิศวกรด้านเครือข่ายและความปลอดภัย (Network & Security Engineer)	มีบทบาทที่เกี่ยวข้องกับยุทธศาสตร์ ICT ทุกด้าน ตั้งแต่สถาปัตยกรรมระบบในภาพรวมและกรอบทิศทางการพัฒนา การออกแบบในรายละเอียดและการดำเนินงาน ไปจนถึงการปฏิบัติงาน อีกทั้งมีหน้าที่ออกแบบระบบ IT และระบบจัดการศูนย์ข้อมูลทั้งหมด ตลอดจนจัดการและจัดระเบียบเครือข่ายปฏิบัติการของศูนย์ข้อมูล

หน้าที่และความเชี่ยวชาญที่กล่าวมาข้างต้นมีความสำคัญมากสำหรับหลายหน่วยงาน เนื่องจากภาครัฐมีงบประมาณจำกัด จึงส่งผลให้บุคลากรที่มีความสามารถเลือกทำงานให้ภาคเอกชนที่ให้ผลตอบแทนมากกว่าหน่วยงานภาครัฐ นอกจากนี้ยังมีบุคลากรที่มีทักษะสูงอีกเป็นจำนวนมากที่ย้ายถิ่นฐานและการทำงานไปสู่ภูมิภาคอื่นของโลกเพื่อโอกาสในเส้นทางอาชีพที่ให้ผลตอบแทนสูงกว่า ส่งผลให้ตลาดแรงงานภายในประเทศไทยขาดแคลนบุคลากรมีทักษะที่เหมาะสม

โครงการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM) สำหรับประเทศไทยมุ่งเน้นการดำเนินงานดังต่อไปนี้

- บ่มเพาะผู้มีทักษะและความสามารถในปัจจุบัน ให้ความมั่นคงต่อหน้าที่การงานและบทบาทในอนาคตของบุคลากรเหล่านั้น สนับสนุนการปรับปรุงหน้าที่บุคลากรในหน่วยงานต่างๆ และในรูปแบบการดำเนินงานในอนาคตที่ภาครัฐสนับสนุน เช่น ศูนย์ข้อมูลระดับกระทรวง ศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน และการบริการโดยภาครัฐ เป็นต้น
- จัดการฝึกอบรม พัฒนาความสามารถ และทบทวนทักษะให้แก่ทรัพยากรบุคคลในปัจจุบันให้มีความพร้อมต่อสถานการณ์ของอุตสาหกรรม มีความรู้และข้อมูลล่าสุดเพื่อเพิ่มประสิทธิภาพการทำงาน
- ภาครัฐกำหนดแผนฝึกอบรมบุคลากร เพื่อพัฒนาคุณภาพและประสิทธิภาพของทรัพยากรบุคคล
- หน่วยงานเปิดกว้างและมุ่งเน้นการสนับสนุนเจ้าหน้าที่ด้วยการฝึกอบรม เช่น การพัฒนาหลักสูตร การจัดหาหลักสูตรการจัดอบรม และการพัฒนาทักษะอย่างต่อเนื่อง เป็นต้น

- หน่วยงานภาครัฐมีหลักแห่งเหตุผล เพื่อใช้ประโยชน์จากทรัพยากรบุคคลที่มีอยู่ให้เกิดประสิทธิภาพในรูปแบบการดำเนินงานในอนาคตที่ได้เลือก เช่น การบริการโดยภาครัฐ ศูนย์ข้อมูลระดับกระทรวง และศูนย์ข้อมูลให้บริการระหว่างหน่วยงาน

การจัดจ้างทรัพยากรบุคคลภายนอกหน่วยงาน (Human Resources Outsourcing หรือ HRO) ยังคงเป็นแนวทางสำคัญในการผลักดันการเติบโตขององค์กร โดยจากผลการสำรวจในปี ค.ศ. 2013 ของ Society for Human Resources Management นั้นได้ระบุ 6 เหตุผลสำคัญของสาเหตุที่หน่วยงานต่างๆ ต้องพึ่งพาการจัดจ้างทรัพยากรบุคคลในวิธีนี้ ซึ่งเหตุผลทั้งหมดมีดังนี้

- ประหยัดต้นทุน
- มุ่งเน้นยุทธศาสตร์
- ยกระดับการปฏิบัติตามกฎต่างๆ
- เพิ่มความถูกต้องแม่นยำ
- บุคลากรมีทักษะและความเชี่ยวชาญ
- การใช้ประโยชน์จากเทคโนโลยี

การจัดจ้างทรัพยากรบุคคลภายนอกหน่วยงาน (HRO) ถือเป็นทางเลือกที่มีบทบาทมากขึ้นอย่างต่อเนื่องสำหรับหน่วยงานภาครัฐ ซึ่งข้อดีของการจัดจ้างดังกล่าวมีดังนี้

- เพิ่มประสิทธิภาพการทำงาน – เจ้าหน้าที่ของหน่วยงานสามารถมุ่งเน้นการทำงานเชิงยุทธศาสตร์มากขึ้น
- เข้าถึงเทคโนโลยีทันสมัย – สามารถใช้งานอุปกรณ์เทคโนโลยีล่าสุด โดยไม่ต้องรับภาระในการเป็นเจ้าของ
- ได้รับความช่วยเหลือจากผู้เชี่ยวชาญด้านข้อมูลในการปฏิบัติตามกฎระเบียบการจ้างงาน – ผู้ให้บริการการจัดจ้างในรูปแบบนี้จะมีจุดแข็งในเรื่องของข้อมูลและการเปลี่ยนแปลงด้านกฎหมายแรงงาน การเรียกร้องสินไหมประกัน และระเบียบข้อบังคับด้านผลประโยชน์แรงงานอยู่เสมอ ซึ่งเป็นการลดภาระของหน่วยงานภาครัฐในหน้าที่ดังกล่าวได้เป็นอย่างดี

การจัดจ้างทรัพยากรบุคคลภายนอกหน่วยงาน เอื้อให้หน่วยงานสามารถพัฒนาศักยภาพในการให้บริการโดยปราศจากภาระการจ้างบุคลากรเพิ่มเติม นอกจากนี้ การจัดจ้างในรูปแบบดังกล่าวยังช่วยลดความเสี่ยงทางการเงินอันเนื่องมาจากการไม่สามารถปฏิบัติตามระเบียบข้อบังคับการจ้างงานของภาครัฐได้

แนวโน้มปัจจุบันและอนาคต

- การย้ายไปใช้งานระบบคลาวด์ การย้ายข้อมูลทรัพยากรบุคคลของหน่วยงานจากเครื่องแม่ข่ายไปจัดเก็บไว้บนระบบคลาวด์กำลังกลายเป็นแนวปฏิบัติมาตรฐานในหลายหน่วยงานภาครัฐ ผู้ให้บริการระบบทรัพยากรบุคคลภายนอกให้เหตุผลว่าระบบคลาวด์มีกระบวนการรักษาความปลอดภัยด้านข้อมูลที่มีประสิทธิภาพสูงกว่าและมีประโยชน์ในแง่ที่เอื้อให้หน่วยงานมีความต่อเนื่องในการดำเนินงาน การจัดจ้างผู้ให้บริการระบบทรัพยากรบุคคลภายนอกองค์กรผ่าน

ระบบคลาวด์มีข้อดีในด้านการจัดทำรายงานและการวิเคราะห์ผล รวมถึงระบบช่วยเหลือพนักงานแบบบูรณาการและบริการด้านทรัพยากรบุคคลอื่นๆ ที่เกี่ยวข้อง

- กระบวนการอัตโนมัติ (Process Automation) จากการใช้งานแพลตฟอร์มทรัพยากรบุคคลบนระบบคลาวด์ กระบวนการอัตโนมัติจะช่วยเพิ่มประสิทธิภาพในการดำเนินงาน ลดความซับซ้อนในการจัดการผลประโยชน์ของเจ้าหน้าที่และพนักงาน และลดภาระหน้าที่จัดการภายใน (Back Office) ที่ต้องอาศัยระบบแรงงานคน (Manual) เป็นได้อย่างมาก
- การจัดจ้างหน่วยงานภายนอกเฉพาะด้าน (Selective Outsourcing) แนวโน้มที่มีมาอย่างต่อเนื่องคือ การจัดจ้างหน่วยงานภายนอกเฉพาะด้าน หน่วยงานจะทำการจัดจ้างเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญเฉพาะด้านจากภายนอก ขณะที่ยังรักษาหน้าที่ส่วนอื่นๆ ไว้ภายในองค์กร วิธีนี้การนี้เป็นแนวทางที่มีประสิทธิภาพในการคัดสรรบุคลากร ทำให้สามารถจัดหาบุคลากรได้อย่างรวดเร็วและทันต่อความต้องการ
- การสรรหาบุคลากรด้วยสื่อสังคม (Social Media Recruiting) ผู้ให้บริการทรัพยากรบุคคลหลายรายกำลังใช้วิธีสรรหาและคัดสรรบุคลากรผ่านสื่อสังคมออนไลน์มากขึ้น เพื่อใช้ประโยชน์สูงสุดจากเทคโนโลยีดังกล่าวที่มีความหลากหลายของบุคลากรที่ให้เลือกสรร

ภาคผนวก ก: แนวทางปฏิบัติด้านนโยบายข้อมูลของการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

ความปลอดภัย (Security)

- บุคลากรที่ปฏิบัติงานร่วมกับภาครัฐ เช่น พนักงาน ผู้รับเหมา และผู้ให้บริการ เป็นต้น มีหน้าที่ต้องรับผิดชอบในการรักษาความลับและปกป้องข้อมูลที่ใช้งาน แม้ข้อมูลนั้นปราศจากการระบุว่าลับหรือไม่ นอกจากนี้ บุคลากรดังกล่าวต้องได้รับการฝึกอบรมอย่างเหมาะสม
- ข้อมูลรั่วไหลโดยอุบัติเหตุหรือความจงใจ และข้อมูลสูญหายหรือถูกนำไปใช้ในทางที่ผิด อาจนำไปสู่ความเสียหายและความผิดทางกฎหมาย บุคลากรมีหน้าที่ปกป้องข้อมูลหรือทรัพย์สินภายใต้การควบคุมดูแล และต้องได้รับคำแนะนำเกี่ยวกับข้อกำหนดด้านความปลอดภัย กฎหมาย และบทลงโทษที่อาจได้รับ
- หน่วยงานและภาครัฐต้องจัดเตรียมระบบจัดการเหตุละเมิดความปลอดภัยให้พร้อม เพื่อรายงานพฤติกรรมที่ไม่เหมาะสม และใช้เป็นหลักฐานในการดำเนินการทางวินัยและทางกฎหมาย

ข้อมูลอ่อนไหว (Sensitive Information)

- การเข้าถึงข้อมูลอ่อนไหวต้องได้รับการอนุญาตบนพื้นฐาน “ความจำเป็นที่ต้องทราบ” เพียงเท่านั้นและต้องมีมาตรการรักษาความปลอดภัย
- ข้อมูลต้องมีความน่าเชื่อถือและความพร้อมใช้งานสำหรับบุคลากรที่ได้รับสิทธิ์เท่านั้น การขาดความสามารถในการใช้ประโยชน์จากข้อมูลเหล่านี้ร่วมกัน เช่น ประวัติผู้ป่วย เป็นต้น อาจส่งผลต่อการดำเนินงานและก่อให้เกิดผลเสียตามมา นอกจากนี้ การเปิดกว้าง (Openness) ความโปร่งใส (Transparency) ข้อมูลเปิด (Open Data) และการนำข้อมูลกลับมาใช้ใหม่ (Reuse) ส่งผลให้การเข้าถึงข้อมูลต้องอาศัยดุลพินิจที่เหมาะสม โดยคำนึงถึงการคุ้มครองข้อมูลและความลับของข้อมูลเป็นสำคัญ
- การรั่วไหล การสูญหาย หรือการใช้ข้อมูลอ่อนไหวผิดวิธีอาจมีผลกระทบร้ายแรงต่อการดำเนินงานของภาครัฐ องค์กร หรือบุคลากร การเข้าถึงข้อมูลอ่อนไหวต้องไม่เกินขอบเขตความจำเป็นในการดำเนินงานของหน่วยงานนั้น โดยควรจำกัดให้เฉพาะผู้ที่ได้รับสิทธิ์ และควรต้องมีการรักษาความปลอดภัยอย่างเหมาะสม โดยหลักการ “ความจำเป็นที่ต้องทราบ” ต้องถูกนำมาใช้หากมีการรวบรวม จัดเก็บ ประมวลผล และแบ่งปันข้อมูลที่มีความอ่อนไหวภายในภาครัฐหรือระหว่างภาครัฐกับเอกชนภายนอกและภาคีระหว่างประเทศ
- ข้อมูลที่มีความอ่อนไหวมากมักส่งผลให้มีความจำเป็นต้องเข้าใจในข้อกำหนดด้านความปลอดภัยมากขึ้น (การปฏิบัติตามกฎข้อบังคับด้านความปลอดภัย) หากในกรณีฉุกเฉินที่ต้องเปิดเผยข้อมูลความอ่อนไหว เช่น เพื่อปกป้องชีวิตหรือเพื่อยุติอาชญากรรมร้ายแรงนั้น เจ้าหน้าที่ควรปกป้องแหล่งที่มาของข้อมูลหากสามารถทำได้ หากเกิดข้อสงสัยในการอนุญาตให้บุคคลใดเข้าถึงข้อมูลอ่อนไหว ให้เจ้าหน้าที่นั้นปรึกษาผู้บังคับบัญชาหรือเจ้าหน้าที่ด้านความมั่นคงปลอดภัยก่อนดำเนินการ และควรบันทึกเวลาและเหตุผลในการกระทำดังกล่าวด้วยทุกครั้ง
- ข้อมูลอ่อนไหวบางประเภทจะมีการแจ้งเตือน (Caveat) เช่น ข้อมูลอ่อนไหวของทางการ เป็นต้น หรือต้องการ

การจัดการเป็นพิเศษ เช่น การใช้ Codeword (คำอธิบายการใช้ Codeword อยู่ในเนื้อหาถัดไป) เพื่อระบุมาตรการควบคุมเพิ่มเติมในการเผยแพร่

- ข้อมูลอ่อนไหวที่กล่าวมา มีการควบคุมเชิงกระบวนการหรือเทคนิคเพิ่มเติมเพื่อ “ความจำเป็นที่ต้องทราบ” นอกจากนี้ จุดประสงค์ของการควบคุมทางเทคนิคคือ เพื่อทำเครื่องหมายแบ่งแยกประเภทของข้อมูล เช่น สำหรับการจัดการการเข้าถึง หรือการจำกัดจำนวนข้อมูลที่ผู้ใช้งานหนึ่งรายสามารถเปิดดูได้ เป็นต้น ซึ่งการควบคุมเหล่านี้จะต้องอาศัยระบบที่สามารถดำเนินการได้อย่างมีประสิทธิภาพ

การคุ้มครองทรัพย์สิน (Asset Protection)

- ทรัพย์สินที่ได้รับหรือแลกเปลี่ยนกับภาคีภายนอกต้องได้รับการคุ้มครองให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง ข้อตกลง หรือพันธกรณีระหว่างประเทศ
- ทรัพย์สินที่ภาครัฐได้รับจากหน่วยงานอื่น เช่น รัฐบาลต่างประเทศ องค์กรสากล องค์กรพัฒนาเอกชน และบุคคลทั่วไปควรได้รับการคุ้มครองให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง ข้อตกลง หรือพันธกรณีระหว่างประเทศอย่างเท่าเทียมเช่นกัน
- ข้อมูลที่ได้รับจากรัฐบาลต่างประเทศหรือองค์กรสากล จะต้องได้รับการคุ้มครองในระดับเทียบเท่ากับข้อมูลความอ่อนไหวของประเทศไทยในระดับเดียวกัน
- ข้อมูลหรือทรัพย์สินอื่นๆ ที่ได้รับจากต่างประเทศ จากองค์กรสากล หรือองค์กรพัฒนาเอกชนไทย ต้องได้รับการคุ้มครองในมาตรฐานเดียวกับทรัพย์สินภาครัฐของไทยเป็นอย่างน้อย หากไม่มีข้อตกลงหรือสัญญาความปลอดภัยร่วมกัน
- ผู้เป็นเจ้าของข้อมูลมีหน้าที่ระบุความอ่อนไหวของข้อมูลและจัดเตรียมกระบวนการที่เหมาะสมเพื่อจัดการข้อมูลนั้นอย่างปลอดภัยและสอดคล้องกับข้อกำหนดทางกฎหมาย ผู้เป็นเจ้าของข้อมูลนี้ควรใช้ดุลยพินิจอย่างเหมาะสมในการกำหนดแนวทางการจัดการข้อมูลอ่อนไหวของตนอย่างมีประสิทธิภาพ
- ในการจัดการข้อมูลอ่อนไหวในระดับต่างๆ หน่วยงานอาจใช้การติดป้าย (Descriptor) เพิ่มเติมควบคู่กับการทำเครื่องหมายแบ่งแยกประเภทของข้อมูล เพื่อจัดการการเข้าถึงข้อมูลที่มีประสิทธิภาพมากขึ้น
- หน่วยงานต่างๆ อาจประยุกต์ใช้การติดป้าย (Descriptor) เพื่อระบุข้อมูลอ่อนไหวที่สำคัญบางประเภทและเพื่อจัดการการเข้าถึงข้อมูล การติดป้าย (Descriptor) ต้องมีนโยบายภายในประเทศรองรับ การติดป้าย (Descriptor) นี้ต้องมีการใช้ร่วมกันกับการจัดระดับความปลอดภัย ซึ่งมีรูปแบบคือ “PUBLIC-SENSITIVE [Descriptor]” เช่น “PUBLIC-SENSITIVE [Finance]” สำหรับข้อมูลการคลัง
- การติดป้าย (Descriptors) ไม่สามารถใช้กับข้อมูลที่ส่งไปยังภาคีต่างประเทศ (เว้นแต่มีการตกลงกันล่วงหน้า) เพราะอาจก่อให้เกิดความสับสนได้

อักษรรหัส (Codeword)

- อักษรรหัส (Codeword) เป็นกลไกรักษาความปลอดภัยแก่ทรัพย์สิน Codeword เป็นคำเดียวในรูปแบบตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ และมักถูกวางไว้ด้านหลังเครื่องหมายจำแนกประเภทของข้อมูล ซึ่งมักใช้กับข้อมูล

อ่อนไหวและข้อมูลความลับเท่านั้น ตัวอย่างเช่น ภาครัฐใช้ ADEF หรือคำใดๆ เป็นอักษรรหัส (Codeword) สำหรับข้อมูลลับ เช่น PUBLIC-SENSITIVE [ADEF] เป็นต้น

การทำงานร่วมกับการจำแนกประเภทความปลอดภัย (Working with Security Classifications)

- การจำแนกประเภทความปลอดภัยสามารถใช้ได้กับข้อมูลทุกชนิดที่มีความสำคัญ ซึ่งรวมถึงข้อมูลในทุกรูปแบบ (ไม่นับรวมระบบเทคโนโลยีสารสนเทศที่ใช้จัดเก็บหรือประมวลผลข้อมูลที่เป็นความลับ) เช่น รายการอุปกรณ์ฮาร์ดแวร์ และทรัพย์สินมีค่าอื่นๆ การทำเครื่องหมายจำแนกประเภทความปลอดภัยควรมองเห็นได้ง่ายและควรระบุวิธีใช้ หน่วยงานต้องมีการควบคุมอย่างเหมาะสมหรือต้องได้รับการแนะนำ ในกรณีที่ไม่สามารถทำเครื่องหมายบนอุปกรณ์ได้ เช่น ทรัพย์สินเปลี่ยนมือง่าย (Inherent Transferable Value) หรืออุปกรณ์ต้องได้รับการดูแลเป็นพิเศษ โดยทรัพย์สินเหล่านี้อาจต้องมีการพิจารณาการดำเนินการเพื่อควบคุมในรูปแบบอื่นๆ
- เมื่อมีการใช้งานทรัพย์สินด้านข้อมูล หน่วยงานควรต้องพิจารณาประเด็นต่อไปนี้
    - ไม่มีข้อบังคับในการทำเครื่องหมายบนทรัพย์สินสาธารณะ
    - การทำเครื่องหมายความปลอดภัยในระดับที่สูงเกินไปอาจเกินความจำเป็น
    - การทำเครื่องหมายความปลอดภัยที่น้อยเกินไปอาจนำไปสู่การควบคุมที่ไม่เหมาะสม ซึ่งก่อให้เกิดความเสี่ยงมากขึ้น
    - เมื่อทำงานเอกสาร การจำแนกประเภทความปลอดภัยควรระบุเป็นตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ที่ด้านบนและด้านล่างของเอกสารทุกหน้า ข้อมูลอ่อนไหวควรแยกใส่ไว้ในภาคผนวกเพื่อให้สามารถเผยแพร่เนื้อหาหลักได้อย่างมีประสิทธิภาพ
    - ต้องมีการทำเครื่องหมายสำหรับข้อมูลอ่อนไหวที่เผยแพร่บนเครือข่ายอินทราเน็ต (Intranet) อย่างชัดเจน
    - ควรมีการระบุว่าเป็นความลับในหัวเรื่องและในข้อความของจดหมายอิเลกทรอนิกส์
    - เจ้าของทรัพย์สินเท่านั้นที่สามารถจำแนกประเภททรัพย์สิน หรือปรับเปลี่ยนการจำแนกประเภททรัพย์สินนั้นได้ นอกจากนี้ ควรมีการหารือกับเจ้าของทรัพย์สินก่อนที่หน่วยงานอื่นจะปรับเปลี่ยนการจำแนกประเภททรัพย์สินนั้นและเผยแพร่ออกไป
    - ไฟล์ เอกสาร หรือทรัพย์สินที่มีความอ่อนไหวต้องมีการทำเครื่องหมายติดไว้ เช่น แฟ้มเอกสาร หรือจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาความลับต้องมีเครื่องหมายกำกับไว้ (เช่น ระบุว่าข้อมูลความลับ)
    - จดหมายอิเล็กทรอนิกส์มักเป็นเอกสารเชิงบทสนทนาที่มีความยาว ดังนั้น ผู้ส่งต่อควรประเมินเนื้อหาทั้งหมดของจดหมายอิเล็กทรอนิกส์เสียก่อนที่จะเพิ่มเติมเนื้อหาและทำการส่งต่อออกไป
    - ในบางสถานการณ์อาจสมควรที่จะเลือกเผยแพร่ข้อมูลอ่อนไหวเฉพาะบางส่วน ผู้ส่งข้อมูลนั้นควรคัดกรองข้อมูลความลับออกก่อนทำการเผยแพร่

การประเมินมูลค่าทรัพย์สินเทคโนโลยี: การรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน (Valuing Technology Assets: Confidentiality, Integrity and Availability)

- เนื่องจากผลกระทบจากการสูญหายของข้อมูลหรือการขาดความพร้อมของระบบต่อการดำเนินงานอาจมีหลายระดับ ดังนั้นภาครัฐควรพิจารณาบริหารความเสี่ยงและป้องกันความเสียหาย
- ควรมีการใช้มาตรการเพื่อลดความเสี่ยงต่อการสูญหายของข้อมูลหรือความไม่พร้อมของระบบ ถึงแม้ว่าผลกระทบอาจมีน้อยก็ตาม
- การรวบรวม การสะสม และการเชื่อมโยงกันของข้อมูลภายในระบบ ICT และอุปกรณ์จัดเก็บข้อมูลต่างๆ ควรมีการบริหารจัดการเพื่อลดความเสี่ยง

ความปลอดภัยเชิงกายภาพ: วิธีประเมินความเสี่ยง (Physical Security: Risk Assessment Methodologies)

- การควบคุมความปลอดภัยทางกายภาพ (Physical Security) ควรนำมาใช้คุ้มครองทรัพย์สินภาครัฐ ซึ่งการประเมินความเสี่ยง (Risk Assessment) จะระบุภัยคุกคามและความเสี่ยงที่อาจเกิดขึ้น
- หากมีความเข้าใจต่อภัยคุกคามข้อมูล ภาครัฐควรจัดทำข้อบังคับการดำเนินงาน (Operational Requirements หรือ OR ซึ่งเป็นวิธีการระบุข้อบังคับด้านความปลอดภัย) ก่อนทำการจัดซื้อหรือใช้งานระบบด้านความมั่นคงปลอดภัย
- ขั้นตอนของ Security Assessment for Protectively Marked Assets (SAPMA) ควรได้รับการดำเนินการให้เสร็จสมบูรณ์เพื่อกำหนดมาตรการควบคุมความปลอดภัยเพิ่มเติมที่เหมาะสำหรับป้องกันหรือตรวจจับการรั่วไหลของข้อมูล และเพื่อคุ้มครองทรัพย์สินจากการโจมตี

หลักการความปลอดภัยของข้อมูล (Information Security Principles)

- ข้อมูลทุกระดับในการจำแนกประเภทควรได้รับการคุ้มครองอย่างเคร่งครัด ซึ่งจำเป็นต่อการสร้างความเชื่อมั่นระหว่างองค์กรต่างๆ และเพื่อเพิ่มระดับการทำงานร่วมกัน
- คณะกรรมการภาครัฐเป็นผู้บริหารความเสี่ยงในภาพรวมสำหรับข้อมูลประเภทต่างๆ โดยภาครัฐต้องจัดตั้งคณะกรรมการเพื่อประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลทั่วไป ข้อมูลสำคัญ และข้อมูลด้านความมั่นคงของประเทศ
- หน่วยงานภาครัฐยังคงเป็นเจ้าของและเป็นผู้จัดการความเสี่ยงด้านข้อมูลของตนเอง หน่วยงานต่างๆ จะประเมินความเสี่ยงของตนและพิจารณาแนวทางการบรรเทาความเสี่ยงอย่างเหมาะสม เพื่อทำให้ความเสี่ยงและการดำเนินงานมีความสมดุลกัน

การพิจารณาการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล (Confidentiality, Integrity and Availability Considerations)

- นโยบายการจำแนกประเภทข้อมูล (Classification Policy) มีความเกี่ยวข้องกับข้อกำหนดการรักษาความลับ นอกจากนี้ การบริการของภาครัฐยังมีข้อกำหนดด้านความสมบูรณ์ข้อมูลและความพร้อมใช้งานที่สำคัญ การนำข้อมูลที่ขาดความสมบูรณ์หรือขาดความพร้อมใช้งานไปใช้ในการประมวลผล อาจมีผลกระทบรุนแรงกว่าความลับรั่วไหล
- ข้อกำหนดความสมบูรณ์หรือความพร้อมใช้งานระดับสูงมิได้หมายถึงการจำแนกประเภทข้อมูลระดับสูง ทั้งนี้ ต้องมีการประเมินความเสี่ยงแบบรอบด้าน เช่น การพิจารณาความเสี่ยงในการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน นอกจากนี้ การปฏิบัติตามข้อกำหนดด้านความสมบูรณ์หรือความพร้อมใช้งานอาจต้องอาศัยมาตรการควบคุมทางเทคนิคและระดับความเชื่อมั่นที่สูงกว่าการจำแนกประเภทความลับ

การรวบรวมข้อมูล (Aggregation)

- เนื่องจากภาครัฐมีการใช้งานระบบร่วมกัน มีการใช้ระบบ ICT เพิ่มขึ้น และมีการให้บริการสาธารณะผ่านช่องทางดิจิทัลมากขึ้น จึงส่งผลให้มีข้อมูลปริมาณมากมารวมอยู่ในไม่เพียงกี่ระบบ หรือมีเพียงแค่ระบบเดียวที่ให้หลายบริการมาใช้ร่วมกัน
- การควบรวมระบบหรือการบริการอาจก่อให้เกิดเงื่อนไขดังต่อต่อไปนี้
    - ผลกระทบต่อการดำเนินงานจากการสูญหาย การรั่วไหล หรือการใช้ข้อมูลที่รวมกันอยู่ในทางที่ผิด มักก่อความเสียหายได้มากกว่าข้อมูลชุดเดียว ซึ่งในบางกรณี ผลกระทบอาจรุนแรงได้ เช่น การสูญหายของข้อมูลเลขประจำตัวประชาชนที่ถูกจัดเก็บไว้
    - ภัยคุกคามข้อมูลที่มีอยู่เดิมอาจมีเพิ่มมากขึ้น เนื่องจากผู้ประสงค์ร้ายต้องการหาผลประโยชน์จากข้อมูลจำนวนมากที่รวมกัน
    - ภัยคุกคามอาจโจมตีชุดข้อมูลหรือการบริการที่รวมกัน เนื่องจากข้อมูลที่รวมกันอาจมีมูลค่ามหาศาล ด้วยเหตุนี้ ผู้ประสงค์ร้ายอาจถือเป็นการโจมตีที่คุ้มค่า
    - ข้อมูลที่รวมกันควรถูกจัดให้อยู่ในระดับการจำแนกประเภทเดียวกัน และต้องมีมาตรการควบคุมดูแลอย่างรอบคอบและเคร่งครัด

การประเมินผลกระทบต่อการดำเนินงาน (Assessing the Impact on the Business)

- ควรหลีกเลี่ยงการรวบรวมข้อมูลไว้ในอุปกรณ์ของผู้ใช้งานหรือส่งข้อมูลไปยังอุปกรณ์ของผู้ใช้งานเกินกว่าที่ข้อกำหนดอนุญาต การหลีกเลี่ยงดังกล่าวจะช่วยลดผลกระทบได้หากมีการรั่วไหลของข้อมูลและการกระทำอันไม่เหมาะสมของผู้ใช้งาน ทั้งนี้ ภาครัฐอาจมีมาตรการควบคุมทางเทคนิคเพื่อจำกัดการเข้าถึงข้อมูลหรือการบริการ หรือมีแนวทางติดตามการทำธุรกรรมเพื่อตรวจจับและป้องกันการเข้าถึงข้อมูลหรือการบริการที่มีพฤติกรรมต้องสงสัย
- ต้องทำการประเมินความเสี่ยง เพื่อกำหนดมาตรการควบคุมทางเทคนิคที่จำเป็นต่อการปกป้องชุดข้อมูล ซึ่ง

ครอบคลุมถึงความเข้าใจว่าการรวบรวมข้อมูลเข้าด้วยกันมีผลกระทบต่อภัยคุกคามอย่างไร มาตรการควบคุมทางเทคนิคได้จัดให้มีไว้เพื่อปกป้องข้อมูลควรมีการดำเนินการอย่างรอบคอบและเจ้าของข้อมูลอาจต้องตัดสินใจว่าจะใช้ระดับความเชื่อมั่นสูงขึ้น หรือใช้ความสามารถทางเทคนิคเพิ่มเติม (เช่น การคงทนต่อความเสียหาย หรือ Fault Tolerance) การประเมินความเสี่ยงสำหรับบริการหรือข้อมูลที่รวบรวมไว้ควรกำหนดมาตรการควบคุมทางเทคนิคที่เหมาะสม

- องค์กรถูกกำหนดให้ประเมินผลกระทบต่อการดำเนินงาน ในกรณีที่เกิดความเสี่ยงด้านข้อมูล การประเมินนี้ควรรวมอยู่ในการประเมินความเสี่ยงในภาพรวม ซึ่งคำนึงถึงภัยคุกคาม ช่องโหว่ และความน่าจะเป็น โดยกระบวนการประเมินความเสี่ยงต้องคำนึงถึง การรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล ซึ่งแยกแต่ละหัวข้อออกจากกัน
- ในแต่ละระดับชั้นของการจำแนกประเภทข้อมูลจะมีขอบเขตข้อมูลที่มีระดับของผลกระทบต่อการดำเนินงานแตกต่างกัน
- โครงสร้าง Business Impact Level (BIL) ควรนำมาประยุกต์ใช้ในกระบวนการประเมินความเสี่ยงด้านข้อมูล แต่ไม่เหมาะสำหรับการทำเครื่องหมายกำกับระบบสารสนเทศหรือการบ่งชี้ระดับการรองรับความน่าเชื่อถือ (Level of Accreditation) เพียงเกณฑ์เดียว ในอนาคตอันใกล้ นโยบาย BIL อาจมีการปรับปรุงแก้ไขเพื่อสร้างกระบวนการประเมินเชิงคุณภาพที่สนับสนุนการจัดลำดับความสำคัญในการดำเนินการ แต่ทั้งนี้ไม่มีความเชื่อมโยงโดยตรงระหว่าง BIL และการจำแนกประเภทใดๆ

ฟังก์ชันการรักษาความปลอดภัย (Security Enforcing Functionality)

เมื่อต้องการความสามารถด้านความมั่นคงปลอดภัยหรือผลิตภัณฑ์ด้านความปลอดภัยจะต้องมีความมั่นใจว่าความสามารถหรือผลิตภัณฑ์นั้นๆ ทำงานได้อย่างมีประสิทธิภาพและให้ระดับการป้องกันเป็นไปตามที่คาดหวังไว้ ดังนั้นผลิตภัณฑ์ทั้งหมดจึงต้องมีระดับของการตรวจสอบที่น่าเชื่อถือหรือการรับประกันที่เหมาะสม ให้สอดคล้องกับประเภทข้อมูลที่ทำการปกป้อง

ข้อกำหนดการจัดการข้อมูล (Data Handling Requirements)

ตารางด้านล่างนี้ระบุแนวทางควบคุมดูแลข้อมูลตามการจำแนกประเภทที่ผู้ใช้งานมีหน้าที่ปฏิบัติตามแนวทางที่สอดคล้องกับการจำแนกประเภทข้อมูล

	ข้อมูลทั่วไป	ข้อมูลสำคัญ	ข้อมูลด้านความมั่นคงของประเทศ
การควบคุมการเข้าถึง (Access Controls)	• การเข้าถึง - ไม่มีข้อจำกัด • การเปลี่ยนแปลงแก้ไข – ต้องได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้ได้รับการแต่งตั้ง	• การเข้าถึงและการเปลี่ยนแปลงแก้ไข – จำกัดเฉพาะผู้ได้รับอนุญาตตามบทบาทในการดำเนินงาน เจ้าของข้อมูลหรือผู้ได้รับอนุญาตเป็นผู้ได้รับสิทธิ์ในการเข้าถึงข้อมูล รวมถึงผู้ที่ได้รับการอนุมัติจากผู้บังคับบัญชา	• การเข้าถึงและการเปลี่ยนแปลงแก้ไข – จำกัดเฉพาะผู้ได้รับอนุญาตตามบทบาทในการดำเนินงาน เจ้าของข้อมูลหรือผู้ได้รับอนุญาตเป็นผู้ได้รับสิทธิ์ในการเข้าถึงข้อมูล รวมถึงผู้ที่ได้รับการอนุมัติจากผู้บังคับบัญชา • การเข้าถึงข้อมูลจะต้องมีการยืนยันตัวบุคคลและได้รับสิทธิ์ • ต้องมีข้อตกลงในการรักษา

	ข้อมูลทั่วไป	ข้อมูลสำคัญ	ข้อมูลด้านความมั่นคงของประเทศ
		• การเข้าถึงข้อมูลจะต้องมีการยืนยันตัวบุคคลและการได้รับสิทธิ์	ความลับ
การทำสำเนาและการพิมพ์ (Copying and Printing)	• ไม่มีข้อจำกัด	• ควรพิมพ์ข้อมูลเมื่อมีความจำเป็นที่เหมาะสมเท่านั้น • การทำสำเนาควรจำกัดให้เฉพาะผู้ที่จำเป็นต้องทราบเท่านั้น • ข้อมูลไม่ควรถูกวางทิ้งไว้บนเครื่องพิมพ์หรือเครื่องโทรสาร • อาจส่งผ่านไปรษณีย์ที่มีความปลอดภัย	• ควรพิมพ์ข้อมูลเมื่อมีความจำเป็นที่เหมาะสมเท่านั้น • การทำสำเนาต้องจำกัดให้เฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูลและได้ลงนามในข้อตกลงรักษาความลับ • ข้อมูลไม่ควรถูกวางทิ้งไว้บนเครื่องพิมพ์หรือเครื่องโทรสาร • สำเนาต้องติดเครื่องหมาย “ลับ” กำกับและต้องใส่ซองจดหมายลับในการจัดส่ง
ความปลอดภัยเครือข่าย (Network Security)	• จัดเก็บข้อมูลไว้บนเครือข่ายสาธารณะโดยแนะนำให้ใช้ Firewall ป้องกัน • การป้องกันขั้นต่ำที่ยอมรับได้คือ การกำหนด ACL บนอุปกรณ์ Router	• กำหนดให้ใช้ Network Firewall สำหรับป้องกัน • การป้องกันขั้นต่ำที่ยอมรับได้ คือ การกำหนด ACL บนอุปกรณ์Router • อินเทอร์เน็ตทั้งหมดหรือ Subnet ที่ไม่มีการป้องกัน เช่น Guest Wireless Networks ต้องไม่สามารถมองเห็นเครื่องแม่ข่ายที่จัดเก็บข้อมูล • จัดเก็บไว้ใน Shared Network Server Subnet โดยใช้กฎ Firewall ร่วมกันสำหรับเครื่องแม่ข่ายอื่น	• ใช้ Network Firewall ป้องกันโดยใช้กฎ "Default Deny" • กำหนดให้ใช้ กำหนด ACL บน Router • อินเทอร์เน็ตทั้งหมดหรือ Subnet ที่ไม่มีการป้องกัน เช่น Guest Wireless Networks ต้องไม่สามารถมองเห็นเครื่องแม่ข่ายที่จัดเก็บข้อมูล • จำเป็นต้องมีกฎ Firewall โดยเฉพาะสำหรับระบบ • ควรทบทวนกฎ Firewall สม่ำเสมอ
ความปลอดภัยระบบ (System Security)	• การจัดการและการรักษาความปลอดภัยระบบต้องดำเนินการตามวิธีปฏิบัติที่เป็นเลิศ (Best Practice) • แนะนำให้ใช้ Host-based Software Firewall	• สำหรับการจัดการและการรักษาความปลอดภัยระบบต้องดำเนินการตามวิธีปฏิบัติที่เป็นเลิศ (Best Practice) ที่เหมาะสมกับ OS ที่ใช้งาน • กำหนดให้ใช้ Host-based Software Firewall • แนะนำให้ใช้ Host-based Software IDS/IPS	• สำหรับการจัดการและการรักษาความปลอดภัยระบบต้องดำเนินการตามวิธีปฏิบัติที่เป็นเลิศ (Best Practice) ที่เหมาะสมกับ OS ที่ใช้งาน • กำหนดให้ใช้ Host-based Software Firewall • แนะนำให้ใช้ Host-based Software IDS/IPS
สภาพแวดล้อมเสมือน (Virtual Environment)	• อาจจัดเก็บข้อมูลไว้ใน Virtual Server • การควบคุมความปลอดภัยอื่นๆ ทั้งหมดนำมาใช้กับทั้ง Host และ Guest Virtual Machines	• อาจจัดเก็บข้อมูลไว้ใน Virtual Server • การควบคุมความปลอดภัยอื่นๆ ทั้งหมดนำมาใช้กับทั้ง Host และ Guest Virtual Machines	• อาจจัดเก็บข้อมูลไว้ใน Virtual Server • การควบคุมความปลอดภัยอื่นๆ ทั้งหมดนำมาใช้กับทั้ง Host และ Guest Virtual Machines • ไม่ควรใช้ Host อยู่ใน

	ข้อมูลทั่วไป	ข้อมูลสำคัญ	ข้อมูลด้านความมั่นคงของประเทศ
		• ไม่ควรใช้ Host อยู่ในสภาพแวดล้อมเดียวกันกับ Guest Virtual Servers ที่จำแนกประเภทความปลอดภัยต่างกัน	สภาพแวดล้อมเดียวกันกับ Guest Virtual Servers ที่จำแนกประเภทความปลอดภัยต่างกัน
ความปลอดภัยทางกายภาพ (Physical Security)	• ระบบต้องถูกล็อกไว้ หรือ ออกจากระบบ (Log-out) เมื่อไม่มีผู้ใช้งาน	• ระบบต้องถูกล็อกไว้ หรือ ออกจากระบบ (Log-out) เมื่อไม่มีผู้ใช้งาน • กำหนดให้จัดวางไว้ในสถานที่ปลอดภัย แนะนำให้ใช้ศูนย์ข้อมูลที่มีความปลอดภัย	• ระบบต้องถูกล็อกไว้ หรือ ออกจากระบบ (Log-out) เมื่อไม่มีผู้ใช้งาน • กำหนดให้จัดวางไว้ในศูนย์ข้อมูลที่มีความปลอดภัย • ต้องมีการเฝ้าติดตามการเข้าออก มีบันทึก และ จำกัดเฉพาะผู้ได้รับอนุญาตตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์
การเข้าถึงระบบจัดเก็บข้อมูลจากระยะไกล (Remote Access to Systems Hosting the Data)	• ไม่มีข้อจำกัด	• จำกัดการเข้าถึงเฉพาะ Local Network หรือ VPN • การเข้าถึงระบบจากระยะไกลโดยหน่วยงานภายนอกสำหรับการช่วยเหลือทางเทคนิค จำกัดเฉพาะการเข้าถึงที่มีการยืนยันตัวตนและเป็นแบบชั่วคราวผ่าน Secure Protocol ทางอินเทอร์เน็ต	• จำกัดการเข้าถึงเฉพาะ Local Network หรือ Secure VPN Group • ไม่อนุญาตให้หน่วยงานภายนอกเข้าถึงจากระยะไกลสำหรับการช่วยเหลือทางเทคนิค • แนะนำให้ใช้ Two-Factor Authentication
การจัดเก็บข้อมูล (Data Storage)	• จัดเก็บข้อมูลในเครื่องแม่ข่ายที่ปลอดภัย • จัดเก็บข้อมูลในศูนย์ข้อมูลที่ปลอดภัย	• จัดเก็บข้อมูลในเครื่องแม่ข่ายที่ปลอดภัย • จัดเก็บข้อมูลในศูนย์ข้อมูลที่ปลอดภัย • ไม่ควรจัดเก็บข้อมูลไว้ใน Workstation หรืออุปกรณ์พกพาส่วนบุคคล	• จัดเก็บข้อมูลในเครื่องแม่ข่ายที่ปลอดภัย • จัดเก็บข้อมูลในศูนย์ข้อมูลที่ปลอดภัย • ไม่ควรจัดเก็บข้อมูลไว้ใน Workstation หรือ อุปกรณ์พกพาส่วนบุคคล (เช่น Laptop) โดยในกรณีจัดเก็บไว้ใน Workstation หรือ อุปกรณ์พกพา จะต้องเข้ารหัสแบบ Whole-Disk Encryption • กำหนดให้เข้ารหัสสื่อสำรองข้อมูล • กระดาษหรือสำเนา ต้องไม่วางทิ้งไว้ในที่ที่ผู้อื่นอาจเห็น โดยต้องเก็บไว้ในสถานที่ปลอดภัย
การรับส่งข้อมูล (Transmission)	• ไม่มีข้อจำกัด	• จะแบ่งปันข้อมูลกับผู้ใช้งานที่กำหนด ในระบบ ICT ของผู้รับข้อมูลที่เหมาะสมและได้รับการรับรองเท่านั้น	• กำหนดให้ต้องเข้ารหัส (เช่น ผ่าน SSL หรือ Secure File Transfer Protocols) • ไม่สามารถรับส่งข้อมูลผ่านทางอีเมล์ เว้นแต่เข้ารหัสและใช้ Digital Signature เพื่อรักษาความปลอดภัย

	ข้อมูลทั่วไป	ข้อมูลสำคัญ	ข้อมูลด้านความมั่นคงของประเทศ
การสำรองข้อมูลและการกู้คืนภัยพิบัติ (Backup/Disaster Recovery)	• กำหนดให้ทำการสำรองข้อมูล แนะนำให้ทำการสำรองข้อมูลทุกวัน	• กำหนดให้ทำการสำรองข้อมูลทุกวัน • แนะนำให้จัดเก็บข้อมูลไว้นอกสถานที่ (Off-site Storage)	• กำหนดให้ทำการสำรองข้อมูลทุกวัน • จัดเก็บข้อมูลไว้ในสถานที่ภายนอกที่ปลอดภัย
การล้างข้อมูลและกำจัดสื่อจัดเก็บข้อมูล (Hard Drives, CDs, DVDs, Tapes, Paper, etc.)	• ไม่มีข้อจำกัด	• นำรายงานกลับมาใช้งานใหม่ • ล้าง/ลบสื่ออิเล็กทรอนิกส์	• ทำลายรายงานเป็นชิ้นเล็กชิ้นน้อย • ทำลายสื่ออิเล็กทรอนิกส์
การฝึกอบรม (Training)	• แนะนำให้ฝึกอบรมสร้างความตระหนักเกี่ยวกับความปลอดภัยโดยทั่วไป	• กำหนดให้ฝึกอบรมสร้างความตระหนักเกี่ยวกับความปลอดภัยโดยทั่วไป • กำหนดให้ฝึกอบรมด้านความปลอดภัยของข้อมูล	• กำหนดให้ฝึกอบรมสร้างความตระหนักเกี่ยวกับความปลอดภัยโดยทั่วไป • กำหนดให้ฝึกอบรมด้านความปลอดภัยข้อมูล • กำหนดให้ฝึกอบรมด้านนโยบายและข้อบังคับที่เกี่ยวข้อง
การตรวจสอบ (Auditing)	• ไม่มีความจำเป็น	• การเข้าระบบโดยใช้รหัสผ่าน (Log-in)	• การเข้าระบบโดยใช้รหัสผ่าน (Log-in) และบันทึกการเปลี่ยนแปลงแก้ไข
อุปกรณ์มือถือ (Mobile Device)	• แนะนำให้ใช้รหัสผ่านป้องกัน • แนะนำให้ล็อกเครื่องเมื่อไม่ใช้งาน	• กำหนดให้ใช้รหัสผ่านป้องกัน • กำหนดให้ล็อกเครื่องเมื่อไม่ใช้งาน	• กำหนดให้ใช้รหัสผ่านป้องกัน • กำหนดให้ล็อกเครื่องเมื่อไม่ใช้งาน • กำหนดให้มีการเข้ารหัส
การกำจัดทิ้งและการทำลาย (Disposal / Destruction)	• กำจัดทิ้งด้วยความระมัดระวังโดยใช้ผลิตภัณฑ์กำจัดที่ได้รับอนุญาต เพื่อป้องกันไม่ให้นำมาประกอบใหม่ได้	• ยืนยันเอกสารเสร็จสมบูรณ์ก่อนทำลายทิ้ง • ใช้อุปกรณ์หรือผู้ให้บริการที่ได้รับอนุญาต	• มีมาตรการควบคุมเพื่อเป็นพยาน/บันทึกการทำลายข้อมูล

ภาคผนวก ข: แนวทางปฏิบัติด้านนโยบายการพัฒนาศูนย์ข้อมูลภาครัฐ (GDCM)

พฤติกรรมภายในศูนย์ข้อมูล (Behavior in Data Center)

- บุคคลที่มาติดต่อศูนย์ข้อมูลต้องปฏิบัติตนอย่างสุภาพขณะอยู่ภายในศูนย์ข้อมูล และระงับการใช้วาจาที่ไม่สุภาพหรือก้าวร้าว
- บุคคลที่มาติดต่อศูนย์ข้อมูลควรสวมรองเท้าและแต่งกายอย่างเหมาะสม
- ห้ามนำ เครื่องดื่มแอลกอฮอล์ สสารควบคุม อาวุธปืน และวัตถุระเบิดเข้ามาภายในบริเวณศูนย์ข้อมูลเป็นอันขาด
- ห้ามรับประทานอาหารและเครื่องดื่มภายในพื้นที่ศูนย์ข้อมูล
- ห้ามสูบบุหรี่หรือดื่มเครื่องดื่มแอลกอฮอล์ในบริเวณอาคารศูนย์ข้อมูลทั้งหมด
- อนุญาตให้ใช้โทรศัพท์มือถือภายในศูนย์ข้อมูลได้ ห้ามใช้วิทยุสื่อสารภายในศูนย์ข้อมูล ไม่อนุญาตให้ถ่ายภาพนิ่ง วิดิทัศน์ หรือบันทึกเสียง
- ผู้มีอายุต่ำกว่า 18 ปีหรือผู้ที่ต้องได้รับการดูแลจากผู้ใหญ่ไม่ได้รับอนุญาตให้เข้ามาภายในศูนย์ข้อมูล หากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าหน้าที่รับผิดชอบศูนย์ข้อมูล
- ห้ามมิให้ผู้ใดก่อเหตุให้เกิดผลเสียหายต่อการทำงานของระบบติดตามสถานะโครงสร้างพื้นฐาน และระบบความปลอดภัยของศูนย์ข้อมูลด้วยวิธีการใดๆ
- ห้ามแบ่งปันข้อมูลกรรมสิทธิ์อย่างเคร่งครัด หากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงาน
- ผู้ให้บริการศูนย์ข้อมูลจะไม่รับจดหมายหรือไปรษณีย์แทนหน่วยงาน ณ ศูนย์ข้อมูล จดหมายหรือไปรษณีย์ทั้งหมดควรส่งไปยังที่ทำการของหน่วยงาน
- ห้ามเก็บรักษาวัสดุติดไฟ เช่น ไม้ กระดาษแข็ง กระดาษลูกฟูก วัสดุพลาสติก วัสดุโฟมหีบห่อ ของเหลว หรือตัวทำละลายไวไฟ ไว้ภายในศูนย์ข้อมูล เว้นแต่เจ้าหน้าที่รับผิดชอบศูนย์ข้อมูลอนุญาตเป็นลายลักษณ์อักษร บุคลากรทุกคนต้องรับทราบและปฏิบัติตามมาตรฐานทุกข้อที่เกี่ยวกับการปฏิบัติงานในศูนย์ข้อมูล
- ภาชนะ กล่อง กระเป๋า แล็ปท็อป กระเป๋าถือ กระเป๋าสะพาย หรืออุปกรณ์ทั้งหมดที่ถือเข้าออกศูนย์ข้อมูลต้องผ่านการตรวจสอบของเจ้าหน้าที่ศูนย์ข้อมูลหรือเจ้าหน้าที่รักษาความปลอดภัย
- ห้ามนำสเกตบอร์ด/สเกต สกู๊ตเตอร์ จักรยาน และพาหนะประเภทอื่น เข้ามาในศูนย์ข้อมูล
- บุคคลภายนอกต้องให้ความร่วมมือและเชื่อฟังคำร้องขออันสมควรทุกประการของเจ้าหน้าที่ศูนย์ข้อมูลขณะที่อยู่ภายในอาคาร รวมทั้งแก้ไขการละเมิดกฎทันทีที่หน่วยงานทราบเรื่อง
- เมื่ออุปกรณ์ตรวจจับควันไฟหรือสัญญาณเตือนอัคคีภัยทำงาน เจ้าหน้าที่หน่วยงานทุกคนต้องเตรียมตัวอพยพออกจากอาคารทันทีและรับฟังคำแนะนำเพิ่มเติมจากเจ้าหน้าที่ศูนย์ข้อมูล

ภาพถ่ายหรือวิดิทัศน์ (Pictures or Video)

- ห้ามใช้กล้องถ่ายภาพ กล้องถ่ายวิดีโอ อุปกรณ์ถ่ายภาพอื่นๆ และอุปกรณ์บันทึกเสียง ภายในศูนย์ข้อมูลโดยมิได้รับอนุญาตจากหน่วยงานหรือกระทรวงเป็นลายลักษณ์อักษร ห้ามบุคคลใดนอกจากเจ้าหน้าที่ศูนย์ข้อมูลที่ได้รับอนุญาตทำการถ่ายภาพหรือบันทึกวิดีโอภายในศูนย์ข้อมูล

- ห้ามมิให้ผู้ใดถ่ายภาพหรือถ่ายวิดีโอของศูนย์ข้อมูล การถ่ายภาพหรือวิดีโอต้องมีการจัดเตรียมล่วงหน้าและปฏิบัติตามข้อบังคับการรักษาความปลอดภัยของศูนย์ข้อมูล
- หากจำเป็นต้องใช้ภาพถ่ายหรือวิดีโอเพื่อการเรียกร้องสินไหมประกันหรือการตลาด ให้ติดต่อผู้ให้บริการศูนย์ข้อมูลเพื่อขอความช่วยเหลือ
- ห้ามใช้กล้องทุกชนิดภายในศูนย์ข้อมูล เว้นแต่มีระบุไว้ในเอกสารแนวทางปฏิบัติการบริการ (Service Guide)

ความปลอดภัยทางกายภาพ (Physical Security)

- ศูนย์ข้อมูลเป็นบริเวณที่มีการรักษาความปลอดภัยการเข้าออก และบริเวณอื่นๆ ของอาคารจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- การเข้าออกโดยทั่วไปสำหรับเจ้าหน้าที่ของหน่วยงานจำกัดเฉพาะพื้นที่ที่ได้รับอนุญาตเท่านั้น
- การรักษาความปลอดภัยประกอบด้วย เจ้าหน้าที่ประจำการตลอดตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ ขั้นตอนลงชื่อเข้าออกทุกกรณี แผนจัดการกุญแจและบัตรเข้าออก กระบวนการอนุญาตเข้าออก และวิธีขออนุญาตเข้าออก
- กล้องรักษาความปลอดภัยใช้เฝ้าติดตามพื้นที่บางส่วนของอาคาร ได้แก่ ห้องโถง พื้นที่ส่วนกลาง พื้นที่อาคารศูนย์ข้อมูล และพื้นที่ผู้ดูแล โดยกล้องทุกตัวมีการเฝ้าติดตามและภาพถ่ายจะถูกเก็บรักษาไว้ หากตรวจพบการละเมิดโดยที่กล้องสามารถจับภาพไว้ได้ จะต้องมีการดำเนินการโดยทันที
- ห้ามยุ่งเกี่ยวหรือสร้างผลกระทบและความเสียหายต่อระบบความมั่นคงและความปลอดภัยภายในศูนย์ข้อมูลอย่างเคร่งครัด
- ห้ามเปิดประตูด้านนอกศูนย์ข้อมูลค้างไว้โดยเด็ดขาด โดยประตูเข้าออกเหล่านี้มีการเฝ้าติดตามและมีสัญญาณเตือน
- ผู้ให้บริการศูนย์ข้อมูลสงวนสิทธิ์ในการเข้าสู่พื้นที่ใดๆ ของศูนย์ข้อมูลในทุกช่วงเวลา เนื่องจากเหตุผลด้านความมั่นคงปลอดภัย

การเข้าออกศูนย์ข้อมูล (Data Center Ingress and Egress)

บุคคลที่เข้าออกศูนย์ข้อมูลต้องปฏิบัติดังนี้

- ถือบัตรประชาชนไทย หรือ หลักฐานยืนยันตัวบุคคลที่รัฐบาลออกให้โดยมีรูปถ่ายชัดเจนสำหรับชาวต่างชาติ เช่น หนังสือเดินทาง เป็นต้น
- ได้รับอนุญาตให้เข้าออกอาคาร
- ลงชื่อเข้าออกอาคารตามกฎระเบียบ
- แสดงป้ายรักษาความปลอดภัย “Visitor” สำหรับบุคคลภายนอกตลอดเวลาที่อยู่ภายในศูนย์ข้อมูล
- คืนป้ายรักษาความปลอดภัยและเครื่องมือของศูนย์ข้อมูลก่อนออกจากอาคาร
- เจ้าหน้าที่ของหน่วยงานจะต้องรับทราบและปฏิบัติตามมาตรฐานทั้งหมดที่เกี่ยวกับการทำงานในศูนย์ข้อมูล

การจัดการสิทธิในการเข้าถึงทรัพยากร (Access List Management)

- กระทรวงและหน่วยงานต่างๆ มีหน้าที่รักษาและปรับปรุงรายการสิทธิในการเข้าถึงทรัพยากรในศูนย์ข้อมูล ผู้จัดการศูนย์ข้อมูลควรได้รับใบคำร้องเป็นลายลักษณ์อักษรเพื่อเพิ่มและลบรายการให้อนุญาตเข้าออกของบุคคล บุคคลที่มีชื่อระบุไว้จะได้รับอนุญาตให้เข้าดำเนินการที่ตู้ หน่วยงานอาจอนุญาตให้เจ้าหน้าที่ ผู้ให้บริการหรือเจ้าหน้าที่เทคนิคเข้าถึงตู้เป็นการชั่วคราว
- ผู้ให้บริการศูนย์ข้อมูล (กระทรวงหรือหน่วยงาน) ยังคงมีหน้าที่รับผิดชอบกิจกรรมต่างๆ ของผู้รับเหมา หรือผู้ให้บริการที่ได้รับอนุญาตอื่นๆ ในลักษณะเดียวกับบุคลากรของหน่วยงาน

พื้นที่ส่วนกลาง (Common Area)

- พื้นที่ส่วนกลางคือห้องโถงและทางเดินในอาคาร
- บุคคลที่ใช้พื้นที่ส่วนกลางจะต้องทิ้งเศษขยะลงในภาชนะรองรับที่จัดไว้
- พื้นที่เตรียมอุปกรณ์ (Staging Area) ไม่เปิดให้เข้าสำหรับบุคคลทั่วไปที่เข้าออกศูนย์ข้อมูล
- ผู้ให้บริการศูนย์ข้อมูลสงวนสิทธิ์ที่จะปฏิเสธการเข้าออกแก่ผู้ที่ใช้พื้นที่ส่วนกลางในทางที่ผิดและรบกวนสิทธิของของบุคคลอื่น

ข้อกำหนดการติดตั้งกรงและตู้ และการเดินสายสัญญาณ (Cage, Cabinet and Cabling Requirements)

- ตู้จะต้องมีความสะอาดและเป็นระเบียบตลอดเวลา พื้นที่ตู้จะต้องไม่ก่อให้เกิดภัยหรืออันตรายใดๆ
- ผู้ให้บริการศูนย์ข้อมูลจะต้องเตรียมการป้องกันในทุกกรณี เพื่อรักษาความปลอดภัยของทรัพย์สินภายในสถานที่ตั้งศูนย์ข้อมูล ประตูตู้จะต้องปิดสนิทอยู่ตลอดเวลา
- ผู้ให้บริการศูนย์ข้อมูลต้องกำจัดวัสดุต้องห้าม ได้แก่ กล่อง ลังไม้ กระดาษลูกฟูก พลาสติก วัสดุหีบห่อโฟม และวัสดุอื่นๆ ที่ไม่จำเป็นกับการทำงานของอุปกรณ์ วัสดุเหล่านี้จะต้องจัดวางไว้ในพื้นที่ที่กำหนดในบริเวณจุดขนของ
- ห้ามเก็บวัสดุติดไฟ เช่น กระดาษแข็ง โฟม หรือกระดาษไว้ภายในตู้
- ห้ามสร้าง “พื้นที่สำนักงาน” ภายในพื้นที่วางเครื่องแม่ข่าย บนพื้นที่ใช้สอยศูนย์ข้อมูล พื้นที่วางเครื่องแม่ข่ายสงวนไว้สำหรับใช้วางตู้และอุปกรณ์ภายในเท่านั้น
- ห้ามถอดอุปกรณ์ขณะที่กำลังทำงานออกจากตู้แร็คโดยเด็ดขาด ไม่ควรแขวนหรือติดตั้งสิ่งใดไว้บนกำแพง ตู้อุปกรณ์ดับเพลิง หรืออุปกรณ์เครือข่าย เว้นแต่ได้รับอนุญาตจากเจ้าหน้าที่ประจำศูนย์ข้อมูล
- ไม่ควรวางสิ่งของไว้ด้านบนตู้หรือบนรางสำหรับระบบสายสัญญาณ
- ห้ามเดินสายสัญญาณตามทางเดินหรือบนพื้นไม่เป็นระเบียบหรือนอกบริเวณที่กำหนดอย่างเด็ดขาด อุปกรณ์ทั้งหมดต้องติดตั้งไว้ในตู้แร็คหรือราง สำหรับระบบสายสัญญาณต้องรองรับสายสัญญาณทั้งหมดระหว่างแถวต่างๆ
- ต้องมีการจัดการสายไฟ ใช้สายรัด และสาย Velcro จัดระเบียบสายสัญญาณในตู้แร็คหรือตู้

- ผู้ให้บริการศูนย์ข้อมูลจะเป็นผู้ทำการติดตั้งและถอดอุปกรณ์ในตู้แร็คแต่เพียงผู้เดียว
- ผู้ให้บริการศูนย์ข้อมูลสงวนสิทธิ์ที่จะปฏิเสธการดำเนินการตามหนังสือสั่งงาน (Change Order) หากพิจารณาแล้วว่าตู้หรือสายสัญญาณไม่เข้ากัน ผู้จัดจำหน่ายที่กระทำผิดจะได้รับแจ้งจากผู้ให้บริการศูนย์ข้อมูลเป็นลายลักษณ์อักษรและผู้จัดจำหน่ายจะต้องแก้ไขโดยทันที
- หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดเกี่ยวกับตู้และการเดินสายสัญญาณจะได้รับการแจ้งและร้องขอให้แก้ไขโดยทันที กำหนดให้หน่วยงานปฏิบัติตามข้อกำหนดเรื่องตู้หรือสายสัญญาณและคิดค่าธรรมเนียมจากค่าเสียเวลาและค่าวัสดุที่การกระทำนี้ก่อขึ้น
- ห้ามผู้ใดปีนขึ้นไปบนตู้หรือกำแพง หากต้องการขึ้นไปบนตู้หรือตู้แร็ค ต้องขอความช่วยเหลือจากเจ้าหน้าที่ศูนย์ข้อมูล
- ไม่ควรทำการเปลี่ยนแปลงหรือแก้ไขพื้นที่ โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้บริการศูนย์ข้อมูลเสียก่อน

แร็คและประตูตู้ (Rack/Cabinet Doors)

- ห้ามผู้ใดถอดหรือเปลี่ยนประตูตู้ของตนเอง คำร้องขอเปลี่ยนประตูจะต้องส่งไปให้เจ้าหน้าที่ที่เกี่ยวข้อง และเมื่อได้รับอนุมัติ เจ้าหน้าที่ปฏิบัติการประจำศูนย์ข้อมูลจะดำเนินการถอดหรือเปลี่ยนประตูตู้ให้
- ในกรณีที่ตู้ของหน่วยงานมีการติดตั้งประตู ประตูนั้นต้องปิดไว้ เมื่อหน่วยงานใช้งานอุปกรณ์เสร็จสิ้น
- หากล็อกหรือประตูเสีย ผู้ให้บริการศูนย์ข้อมูลควรติดต่อช่างซ่อมกุญแจที่ได้รับอนุญาต เพื่อขอความช่วยเหลือ ไม่ควรหัก งอ หรือใช้กำลังเปิดประตูออกเอง

กระเบื้องปูพื้น (Floor Tiles)

- ห้ามเจ้าหน้าที่ศูนย์ข้อมูลยกหรือขยับกระเบื้องปูพื้น พื้นที่ใต้พื้นยก (Sub-Floor Area) คือพื้นที่หวงห้าม ซึ่งเข้าออกได้เฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น แผ่นพื้นยกแบบเจาะรูจะวางไว้ตามรูปแบบการทำความเย็น HVAC หากเกิดปัญหาเกี่ยวกับอุณหภูมิ ผู้ให้บริการศูนย์ข้อมูลควรแจ้งผู้ให้บริการด้านระบบทำความเย็นทราบเพื่อแก้ไขปัญหา

อุปกรณ์ศูนย์ข้อมูล (Data Center Equipments)

- อุปกรณ์ศูนย์ข้อมูล เช่น เครื่องมือ รถเข็นล้อเลื่อน รถลาก ลิฟต์ยกเครื่องแม่ข่าย มอนิเตอร์ และ คีย์บอร์ด จะมีให้บริการแก่หน่วยงาน หน่วยงานมีหน้าที่รับผิดชอบอุปกรณ์ที่ยืมทั้งหมดระหว่างที่นำมาใช้งาน และจะต้องคืนอุปกรณ์ทันทีหลังใช้งานเสร็จ
- ไม่อนุญาตให้ปรับเปลี่ยนแก้ไขอุปกรณ์ที่ยืมมาจากศูนย์ข้อมูล หากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้บริการศูนย์ข้อมูล

การรับอุปกรณ์ (Receiving)

- อุปกรณ์จำนวนมาก การขนส่งสินค้า หรืออุปกรณ์ขนาดใหญ่ จะต้องเข้าสู่ศูนย์ข้อมูลผ่านทางบริเวณจุดขนของหรือจุดรับของ (Shipping/Receiving Dock)
- อุปกรณ์ที่ถือเข้ามายังศูนย์ข้อมูลและต้องทำการติดตั้งอาจต้องอาศัยความช่วยเหลือจากเจ้าหน้าที่เทคนิค เพื่อช่วยคำนวณปริมาณการใช้พลังงานและน้ำหนักเพิ่มเติมของอุปกรณ์ชิ้นใหม่ที่ติดตั้งไว้ในตู้แร็ค ความช่วยเหลือลักษณะนี้ทำให้มั่นใจว่าการให้บริการสามารถดำเนินการได้อย่างมีคุณภาพ สอดคล้องกับ SLA ที่กำหนดไว้
- อุปกรณ์ทั้งหมดที่เข้ามายังศูนย์ข้อมูลจะต้องติดชื่อหน่วยงานกำกับไว้ อุปกรณ์ที่ไม่สามารถระบุเจ้าของได้ถือเป็นความเสี่ยงด้านความปลอดภัย อุปกรณ์ลักษณะนี้จะถูกปฏิเสธ เนื่องด้วยเหตุผลด้านความปลอดภัย
- เจ้าหน้าที่ผู้ให้บริการศูนย์ข้อมูลจะต้องไม่เคลื่อนย้ายอุปกรณ์ของหน่วยงานที่ยังไม่แกะหีบห่อหรือยกออกจากรถเข็น (เช่น ตู้ และเครื่องแม่ข่าย เป็นต้น) หน่วยงานเป็นผู้มีหน้าที่แกะหีบห่อ ยกออกจากรถเข็น และ ขยับอุปกรณ์หนักไปยังพื้นที่ศูนย์ข้อมูล รวมถึงค่าใช้จ่ายที่เกี่ยวข้อง หน่วยงานอาจได้รับความช่วยเหลือ เพื่อขนย้ายอุปกรณ์ที่มีน้ำหนักเกินกว่า 45 กิโลกรัม (100 ปอนด์) โดยขึ้นอยู่กับดุลยพินิจของผู้ดูแลศูนย์ข้อมูล
- ต้องมีการดำเนินแผนป้องกันอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อโครงสร้างพื้นฐานด้านข้อมูล

การขนย้ายอุปกรณ์เมื่อสิ้นสุดสัญญาการให้บริการ (Removal of Equipment at End of Term)

- หน่วยงานจะต้องย้ายฮาร์ดแวร์ทั้งหมดออกจากศูนย์ข้อมูลไม่เกินกว่าวันถึงกำหนดสิ้นสุด (Effective Cancellation Date) เว้นแต่มีการตกลงกันเป็นลายลักษณ์อักษร
- หน่วยงานต้องอ้างอิงถึงแนวทางปฏิบัติการบริการ (Service Guide) สำหรับแนวทางปฏิบัติในการยกเลิกสัญญา (Cancellation Guidance)

รางปลั๊กของผู้ใช้บริการ (User Provided Power Strips)

- ห้ามหน่วยงานเสียบรางปลั๊กของตนเองเข้ากับศูนย์ข้อมูล ซึ่งเป็นการละเมิดระเบียบด้านไฟฟ้าและความปลอดภัยและผู้ให้บริการสงวนสิทธิ์ที่จะเรียกร้องให้ถอดอุปกรณ์ออกจากศูนย์ข้อมูล การละเมิดนโยบายนี้จะต้องทำการแก้ไขภายใน 1 วันทำการ หากไม่สามารถแก้ไขการละเมิดกฎนี้ภายใน 1 วันทำการถือเป็นการละเมิดเงื่อนไขในสัญญาของผู้ใช้บริการ

การเพิ่มอุปกรณ์รักษาความมั่นคงปลอดภัยที่เป็นของผู้ใช้ยริการ (User Provided Additional Security Devices)

- หน่วยงานมิได้รับอนุญาตให้เพิ่มอุปกรณ์ความปลอดภัยที่จะกีดขวางการเข้าถึงตู้ของหน่วยงาน โดยตามเหตุผลด้านความมั่นคงและความปลอดภัย หน่วยงานจะต้องสามารถเข้าถึงพื้นที่ทั้งหมดของศูนย์ข้อมูลได้ตลอดเวลา