แผนการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สขญ. ปีงบประมาณ พ.ศ. 2569 - 2570

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) หรือ สขญ. เป็นหน่วยงานของรัฐ ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีเป้าหมายเพื่อเป็นองค์กรหลักในการขับเคลื่อนประเทศด้วยข้อมูลขนาดใหญ่ (Big Data) ให้เกิดการบูรณาการการทำงานระหว่างหน่วยงานภาครัฐและเอกชน ผ่านการนำเทคโนโลยีที่ทันสมัยและองค์ความรู้ด้านข้อมูลมาประยุกต์ใช้เพื่อบริหารจัดการข้อมูลให้เกิดประโยชน์สูงสุด และใช้ข้อมูลเป็นเครื่องมือสำคัญในการขับเคลื่อนนโยบาย เพิ่มศักยภาพการบริหารงานภาครัฐและการดำเนินงานขององค์กร พร้อมทั้งเตรียมความพร้อมให้ประเทศไทยสามารถแข่งขันและปรับตัวต่อการเปลี่ยนแปลงของโลกดิจิทัลในอนาคตได้อย่างมีประสิทธิภาพ และยกระดับคุณภาพชีวิตของประชาชนอย่างยั่งยืน

ในยุคเศรษฐกิจและสังคมที่ขับเคลื่อนด้วยเทคโนโลยีดิจิทัล ในฐานะหน่วยงานของรัฐ มีความจำเป็นต้องปรับปรุงการดำเนินงานขององค์กรให้อยู่ในรูปแบบที่ตอบสนองตอความต้องการของภาคประชาชนและภาคธุรกิจที่เปลี่ยนไป โดยการปรับเปลี่ยนสูการเปนรัฐบาลดิจิทัล

ทั้งนี้ สขญ. จึงได้จัดทำแผนปฏิบัติการ ระยะ 2 ปี (พ.ศ. 2569 – 2570) เพื่อการยกระดับการดำเนินงานและการบริหารจัดการองค์กรด้วยเทคโนโลยีดิจิทัล สำหรับเป็นแนวทางการดำเนินงานที่จะผลักดันสู้การเป็นรัฐบาลดิจิทัล ซึ่งแผนปฏิบัติการ ประกอบด้วย 8 ด้าน ดังนี้

ด้านที่ 1 การปรับเปลี่ยนกระบวนการทำงานของหน่วยงานเป็นดิจิทัล

ด้วย สขญ. ในฐานะที่เป็นหน่วยงานภาครัฐ ได้เล็งเห็นถึงความสำคัญของการปรับเปลี่ยนกระบวนงานเพื่อนำไปสู่การเป็นองค์กรดิจิทัล และสอดคล้องกับแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2560 – 2570 เพื่อให้ทันต่อยุคเศรษฐกิจและสังคมที่ขับเคลื่อนด้วยเทคโนโลยีดิจิทัล การเพิ่มความสามารถและศักยภาพในการแข่งขันของภาคธุรกิจ การสร้างความโปร่งใส ทั้งนี้ จึงได้วางแผนการทำงานภายในองค์กรที่สอดคล้อง โดยมีรายละเอียดดังนี้

1. พัฒนาระบบสารสนเทศพื้นฐานให้สอดคล้องกับการดำเนินงานของสถาบัน เพื่ออำนวยความสะดวกในการปฏิบัติงานของบุคลากรภายในสถาบันทุกมิติ รวมทั้งช่วยลดระยะเวลาในการทำงาน
2. บูรณาการข้อมูลสารสนเทศของแต่ละฝ่ายให้สามารถใช้งานร่วมกันอย่างมีประสิทธิภาพ เพื่อศึกษาและออกแบบโครงสร้างระบบคลังข้อมูล เพื่อให้สอดคล้องกับการดำเนินงานของสถาบัน โดยการประสานงานให้เกิดการทำงานร่วมกันอย่างเป็นระบบ
3. สร้างความตระหนักรู้และเสริมสร้างความปลอดภัยด้านไซเบอร์ให้แก่เจ้าหน้าที่สถาบัน เพื่อสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ เตรียมความพร้อมโดยการจัดทำหลักสูตรทดสอบ และฝึกอบรมบุคลากรภายในให้มีความรู้ความสามารถเพื่อป้องกันการโจมตีทางไซเบอร์และภัยคุกคามที่อาจเกิดขึ้น

โดย สขญ. จะส่งเสริมสนับสนุนการนำนวัตกรรมด้านเทคโนโลยีดิจิทัล เช่น AI, Chat GPT, Data Analytics, Digital ID และอื่นๆ ที่เหมาะสม เพื่อนำมาใช้ในการพัฒนาเศรษฐกิจและสังคมและช่วยแก้ไข

ปัญหาหรือส่งเสริมให้เกิดการพัฒนาด้านต่าง ๆ ที่ดีขึ้นภายในหน่วยงาน รวมทั้งมุ่งเน้นให้เกิดการนำทรัพยากรของหน่วยงาน ทั้งในส่วนขององค์ความรู้ของบุคลากร งบประมาณ ข้อมูล อุปกรณ์ เครื่องมือพิเศษ และวิธีการจัดการต่าง ๆ ไปพัฒนานวัตกรรมที่เป็นประโยชน์กับหน่วยงานรองรับการปฏิบัติงานของบุคลากรในหน่วยงาน โดยคำนึงถึงความสะดวก รวดเร็ว เข้าถึงง่าย เท่าเทียม ลดความซ้ำซ้อนของกระบวนการและข้อมูล อันจะนำไปสู่การขับเคลื่อนการเป็นรัฐบาลดิจิทัล เช่น Work From Anywhere (WFA), การยืนยันตัวตนด้วย Digital ID, การลดใช้กระดาษ โดยมีแผนงาน ดังนี้

1. จัดหาเครื่องมืออุปกรณ์ที่ทันสมัยสนับสนุนการปฏิบัติงานและวิเคราะห์ข้อมูล เพื่อส่งเสริมการสร้างสรรค์นวัตกรรมในองค์กรเช่น การพัฒนาต้นแบบ การพัฒนาระบบ หรือบริการดิจิทัลต่างๆ เพื่อรองรับการปฏิบัติงานของหน่วยงาน
2. จัดหาหรือประยุกต์ใช้เทคโนโลยี เพื่อใช้ในการเพิ่มประสิทธิภาพการทำงานและวิเคราะห์ข้อมูล (Data Analytics) เช่น การประยุกต์ใช้ AI Chatbot หรือ Machine Learning
3. เพื่อให้เกิดการสนับสนุนการทำงานแบบ Paperless หน่วยงานควรดำเนินการ ดังนี้
    - ดำเนินการเปลี่ยนแปลงข้อมูลให้อยู่ในรูปแบบดิจิทัล (Digitize) จัดเก็บเอกสารที่เกี่ยวข้องกับการปฏิบัติงานจากเอกสารให้อยู่ในรูปแบบอิเล็กทรอนิกส์ โดยคำนึงถึงความปลอดภัยของข้อมูล ในการจัดเก็บและทำลายให้เป็นไปตามกฎระเบียบที่เกี่ยวข้อง
    - ดำเนินการใช้ข้อมูลดิจิทัลอย่างเต็มรูปแบบ (Digitalize)
    - มีระบบสารบรรณอิเล็กทรอนิกส์ (ระบบ e-Document)
    - มีระบบ e-Office และ back-Office
    - ใช้ระบบ ThaID เพื่อยืนยันตัวบุคคลในการเข้าถึงทรัพยากรด้านสารสนเทศ และใช้ในการบูรณาการเชื่อมโยงระบบเข้าด้วยกันได้อย่างมีประสิทธิภาพ เพื่อให้เป็นมาตรฐานเดียวกันและมีความมั่นคงปลอดภัย
4. Go Cloud First ซึ่งเป็นนโยบายการใช้บริการและทรัพยากรคอมพิวเตอร์แบบคลาวด์ (Cloud Computing) เป็นหลักสำหรับการพัฒนาโครงสร้างพื้นฐาน ซึ่งประโยชน์ในการใช้เทคโนโลยี Cloud โดยการเช่าใช้บริการทดแทนการจัดหาอุปกรณ์ (Hardware) และโปรแกรม (Software) นั้นมีประโยชน์หลายด้าน เช่น
    - ลดต้นทุนการจัดเก็บและประมวลผลข้อมูลระบบ Cloud ช่วยลดความจำเป็นในการซื้อและบำรุงรักษาฮาร์ดแวร์และซอฟต์แวร์ ซึ่งส่งผลดีต่อต้นทุนขององค์กร
    - เพิ่มประสิทธิภาพองค์กรสามารถปรับขนาดและขยายโครงสร้างพื้นฐานดิจิทัลได้ตามความต้องการ ซึ่งส่งผลดีต่อประสิทธิภาพในการทำงานขององค์กร
    - เพิ่มความยืดหยุ่น ช่วยให้องค์กรสามารถเข้าถึงข้อมูลและระบบบริการได้จากทุกที่และทุกอุปกรณ์ ซึ่งส่งผลดีต่อความยืดหยุ่นในการทำงานขององค์กร
    - เพิ่มความปลอดภัย มีระบบความปลอดภัยที่มีประสิทธิภาพ ซึ่งส่งผลดีต่อความปลอดภัยของข้อมูลและระบบไอทีขององค์กร

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• ใช้คลาวด์เป็นหลัก (Go Cloud First) ไม่น้อยกว่าร้อยละ 70	• ใช้คลาวด์เป็นหลัก (Go Cloud First) ไม่น้อยกว่าร้อยละ 80
	• ปรับปรุงระบบจัดการทรัพยากรองค์กร (ERP) ให้สอดคล้องทันสมัยกับการดำเนินงานของสถาบัน และมีระบบ ERP ใช้งานอย่างต่อเนื่อง	
	• มีระบบ Payroll ใช้งานได้อย่างต่อเนื่อง	
	• ปรับปรุงระบบอิเล็กทรอนิกส์ (e-saraban) ให้สอดคล้องกับการดำเนินงานของสถาบัน สามารถใช้งานได้ต่อเนื่อง ไปในแนวทาง Paperless โดย มีการปรับเปลี่ยนกระบวนงานให้เป็นรูปแบบ Paperless เพื่อรองรับการทำงานบนดิจิทัลแพลตฟอร์ม ไม่น้อยกว่า ร้อยละ 90	• ปรับปรุงระบบ อิเล็กทรอนิกส์ (e-saraban) ให้สอดคล้องกับการดำเนินงานของสถาบัน สามารถใช้งานได้ต่อเนื่อง ไปในแนวทาง Paperless โดยมีการปรับเปลี่ยนกระบวนงานให้เป็นรูปแบบ Paperless เพื่อรองรับการทำงานบนดิจิทัลแพลตฟอร์ม ไม่น้อยกว่าร้อยละ 95
	• ปรับปรุงระบบบริหารงานบุคคล (e-HR) เพื่อช่วยการจัดการข้อมูลในด้านทรัพยากรงานบุคคลให้สอดคล้องกับการใช้งานอย่างมีประสิทธิภาพ	
	• ทบทวนปรับปรุงระบบคลังข้อมูล (Data Warehouse) ของสถาบันให้สอดคล้องกับความต้องการของผู้ใช้งานในแต่ละฝ่าย ทันสมัย ส่งเสริมการสร้างสรรค์นวัตกรรมในองค์กร	• ทบทวนปรับปรุงระบบคลังข้อมูล (Data Warehouse) ของสถาบันให้สอดคล้องกับความต้องการของผู้ใช้งานในแต่ละฝ่าย ทันสมัย ส่งเสริมการสร้างสรรค์นวัตกรรมในองค์กร พร้อมพัฒนาเพื่อส่งเสริมการทำงาน โดยนำ Machine Learning หรือ AI มาช่วยในการวิเคราะห์ข้อมูลให้มีประสิทธิภาพ ส่งเสริมการบริหารจัดการที่มีประสิทธิภาพมากขึ้น
	• มีระบบ eMeeting สามารถทำงานร่วมการยืนยันตัวตนด้วย ThaID ใช้งานได้ต่อเนื่อง	
	• มีระบบ รายงาน ติดตามปัญหา (Incident & Service Management) เพื่อ จัดการให้มีความต่อเนื่องในการให้บริการ (Service Level Agreement: SLA) ดิจิทัลแพลตฟอร์ม ไม่น้อยกว่าร้อยละ 99.90	• มีระบบ รายงาน ติดตามปัญหา (Incident & Service Management) เพื่อ จัดการให้มีความต่อเนื่องในการให้บริการ (Service Level Agreement: SLA) ดิจิทัลแพลตฟอร์ม ไม่น้อยกว่าร้อยละ 99.96
	• ทบทวนปรับปรุงระบบสนับสนุนการทำงานแบบ Work From Anywhere เพื่อใช้ในการบันทึกการทำงาน และประเมินผล (Jira)	

ปีงบประมาณ	ปี 2569	ปี 2570
	• มีการประยุกต์ใช้ AI Chatbot เพื่อให้ข้อมูลภายในกับเจ้าหน้าที่ เพื่อให้สะดวกในการค้นหาข้อมูล	
	• สร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ให้กับบุคลากรทุกระดับในองค์กรอย่างต่อเนื่อง อย่างน้อย 2 ครั้งต่อปี และเสริมสร้างความปลอดภัยในระบบสารสนเทศเพื่อป้องกันการโจมตีทางไซเบอร์และภัยคุกคามที่อาจเกิดขึ้น	

ด้านที่ 2 การมีช่องทางรับฟังและแลกเปลี่ยนความคิดเห็นกับทุกภาคส่วนเพื่อร่วมออกนโยบายและทำประชามติ

สขญ.ได้รับการจัดตั้งขึ้น โดยมีวัตถุประสงค์ข้อหนึ่งในการจัดตั้งตามมาตรา 7 (1) แห่งพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. 2566 คือ “จัดทำยุทธศาสตร์เกี่ยวกับการขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่เพื่อผลักดันให้เกิดการพัฒนาศักยภาพและยกระดับเศรษฐกิจและสังคมของประเทศเพื่อเสนอต่อคณะรัฐมนตรี”การจัดทำยุทธศาสตร์ดังกล่าวจึงเป็นวาระสำคัญของประเทศไทย ที่ สขญ. ได้รับมอบหมายให้ดำเนินการ ซึ่งกระบวนการที่ สขญ. จะต้องดำเนินการเพื่อกำหนดยุทธศาสตร์และแนวทางในการขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ (Big Data) จำเป็นจะต้องรับฟังข้อมูล ความคิดเห็น และข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย ซึ่งครอบคลุมผู้เล่นจากทุกภาคส่วนในระบบนิเวศด้านข้อมูลให้ครบถ้วนตลอดทั้งห่วงโซ่คุณค่า ตลอดจนจะต้องรับฟังประเด็นปัญหา โจทย์การพัฒนา และความต้องการใช้ข้อมูลเชิงวิเคราะห์จากผู้ใช้งานข้อมูล ไม่ว่าจะเป็นหน่วยงานรัฐ เอกชน และประชาชนทั่วไป เพื่อให้ สขญ. สามารถกำหนด focused sector หรือ agenda issue ที่ควรจะมีการบูรณาการและวิเคราะห์ข้อมูลเพื่อให้ตอบโจทย์แบบมุ่งเป้าได้อย่างตรงจุดและเกิดประสิทธิภาพสูงสุดได้ ดังนั้น เพื่อเป็นการเปิดโอกาสให้ทุกภาคส่วนได้มีส่วนร่วมในการกำหนดยุทธศาสตร์การขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ รวมถึงการออกแบบนโยบายทั้งตามรายประเด็นการพัฒนา รายสาขา หรือรายพื้นที่ สำหรับการดำเนินงานด้านข้อมูลของ สขญ. และของรัฐบาลในภาพรวม นั้น สขญ. ควรจะมีการจัดทำช่องทางในการรับฟังและแลกเปลี่ยนความคิดเห็นเพื่อให้หน่วยงานที่เกี่ยวข้องและประชาชนทั่วไป สามารถมีส่วนร่วมในการให้ข้อมูล ความคิดเห็นและข้อเสนอแนะ เพื่อ สขญ. นำมาใช้ประกอบการกำหนดนโยบายและแผนงานในอนาคต ซึ่งต้องเป็นช่องทางที่สะดวก เข้าถึงและใช้งานได้ง่าย และหน่วยงาน/ประชาชนทุกกลุ่มสามารถเข้าถึงได้ในวงกว้าง ดังนั้น สขญ. จึงได้กำหนดแผนงานและเป้าหมายในการจัดทำช่องทางออนไลน์เพื่อการมีส่วนร่วมของทุกภาคส่วน สำหรับปี 2569 - 2570 ไว้ดังต่อไปนี้

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• จัดทำช่องทางออนไลน์เพื่อเปิดให้ประชาชนทั่วไปและหน่วยงานทุกภาคส่วนแสดงความคิดเห็นและข้อเสนอแนะเพื่อการจัดทำแผนยุทธศาสตร์การขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ สำหรับระยะปี พ.ศ. 2571 – 2575	• จัดทำช่องทางออนไลน์เพื่อรับฟังความคิดเห็นและข้อเสนอแนะจากหน่วยงานที่เกี่ยวข้องต่อ(ร่าง) แผนยุทธศาสตร์การขับเคลื่อนการใช้ประโยชน์จากข้อมูลขนาดใหญ่ ระยะปี พ.ศ. 2571 – 2575

ด้านที่ 3 การจัดทำข้อมูลตามหลักธรรมาภิบาลข้อมูลภาครัฐ พร้อมส่งเสริมการเชื่อมโยง แลกเปลี่ยนข้อมูล เปิดเผยข้อมูล และการนำข้อมูลไปใช้ในการวิเคราะห์เชิงนโยบาย

การดำเนินงาน สขญ. ให้ความสำคัญกับการใช้ประโยชน์จากข้อมูลต่าง ๆ ที่ถือเป็นสินทรัพย์ของหน่วยงาน โดยส่งเสริมและผลักดันตั้งแต่เริ่มต้นกระบวนการ ด้วยการจัดทำข้อมูลให้อยู่ในรูปแบบดิจิทัลเพื่อรองรับการแลกเปลี่ยน การบูรณาการ เชื่อมโยงข้อมูล การวิเคราะห์ข้อมูลเพื่อใช้ ในการบริหารจัดการและให้บริการได้อย่างถูกต้องมีประสิทธิภาพ เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จนถึงกระบวนการส่งเสริมให้หน่วยงานเปิดเผยข้อมูลผ่านศูนย์กลางข้อมูลเปิดภาครัฐ เพื่อให้ประชาชนสามารถตรวจสอบการทำงานและเพื่อให้เกิดความโปร่งใสในทุกขั้นตอน โดยมี แผนงาน ดังนี้

1. การสร้างมาตรฐานการบูรณาการเชื่อมโยงข้อมูล ให้เป็นมาตรฐานสากลทั้งในหน่วยงานและระหว่างหน่วยงาน
2. ใช้ประโยชน์ของข้อมูลขนาดใหญ่ รวมกับเทคโนโลยีสมัยใหม่ เพื่อนำมาวิเคราะห์และเชื่อมโยง เพื่อให้เกิดการบูรณาการข้อมูล และให้เกิดประโยชน์สูงสุดต่อทุกภาคส่วน

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• มีการบูรณาการเชื่อมโยงข้อมูลเป็นไปตามมาตรฐานที่กำหนดและหลักธรรมาภิบาลข้อมูลภาครัฐ	• มีการบูรณาการเชื่อมโยงข้อมูลเป็นไปตามมาตรฐานที่กำหนดและหลักธรรมาภิบาลข้อมูลภาครัฐ
	• รูปแบบไฟล์ของชุดข้อมูลเปิดเป็นไปตามเกณฑ์ที่กำหนดเฉลี่ยอย่างน้อยระดับ 3 ดาว : CSV / ODS / XML / JSON / KML / SHP /KMZ	รูปแบบไฟล์ของชุดข้อมูลเปิดเป็นไปตามเกณฑ์ที่กำหนดเฉลี่ยอย่างน้อยระดับ 4 ดาว : RDF (URIs)
	• เผยแพร่และแลกเปลี่ยนข้อมูลเปิดภาครัฐ (Open Data) ผ่านบริการ เช่น ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data) และ ศูนย์กลางแลกเปลี่ยนข้อมูล	• เผยแพร่และแลกเปลี่ยนข้อมูลเปิดภาครัฐ (Open Data) ผ่านบริการ เช่น ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data) และ ศูนย์กลางแลกเปลี่ยนข้อมูล

ปีงบประมาณ	ปี 2569	ปี 2570
	ของภาครัฐ (Government Data Exchange Center)	ของภาครัฐ (Government Data Exchange Center)
	• ใช้ประโยชน์ของข้อมูลขนาดใหญ่ ในการเพิ่มศักยภาพการบูรณาการและวิเคราะห์ข้อมูล เพื่อประกอบการตัดสินใจในการกำหนดนโยบายด้านต่างๆ	• ใช้ประโยชน์ของข้อมูลขนาดใหญ่ ในการเพิ่มศักยภาพการบูรณาการและวิเคราะห์ข้อมูล เพื่อประกอบการตัดสินใจในการกำหนดนโยบายด้านต่างๆ

ด้านที่ 4 การเปิดเผยข้อมูลแก่สาธารณะโดยที่ประชาชนไม่ต้องร้องขอ

การดำเนินงาน สขญ. ในการเปิดเผยข้อมูลเปิดภาครัฐ เป็นการเปิดเผยข้อมูลข่าวสารของราชการในรูปแบบดิจิทัลต่อสาธารณะ โดยผ่านศูนย์กลางข้อมูลเปิดภาครัฐ เพื่อเปิดเผยแก่ประชาชนและมีการกำหนดให้มีมาตราฐานหลักเกณฑ์การเปิดเผยข้อมูลเป็นไปตามหลักการ และแนวทางของคณะกรรมการพัฒนารัฐบาลดิจิทัล โดยจัดทำชุดข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ และเผยแพร่ข้อมูลเปิดภาครัฐบนศูนย์กลางข้อมูลเปิดภาครัฐ (https://data.go.th/) ตามรายชื่อชุดข้อมูลที่ สขญ. สามารถเปิดเผยได้โดยมีขั้นตอน สรุปดังนี้

1. จัดทำบัญชีข้อมูลภายในหน่วยงาน ระบุชุดข้อมูล และจัดระดับความสำคัญของข้อมูลเป็ดภาครัฐที่จะนำไปเปิดเผยตามหน้าที่หรือภารกิจของหน่วยงานของรัฐ
2. จำแนกหมวดหมู่ กำหนดและจัดระดับชั้นข้อมูล โดยพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ
3. กำหนดรูปแบบของชุดข้อมูลของข้อมูลเปิดภาครัฐ อย่างน้อยให้อยู่ในรูปแบบคุณลักษณะแบบเปิด (Open Format) ที่ไม่ขึ้นกับแพลตฟอร์ม หรือไม่จำกัดสิทธิโดยบุคคลใด (Non-proprietary)สามารถอ่านได้ด้วยเครื่อง (Machine Readable) โดยควรมีระดับการปิดเผยชุดข้อมูลอย่างน้อย ระดับ 3 ดาวขึ้นไป และจัดทำคำอธิบายชุดข้อมูลดิจิทัลเพื่อให้ทราบรายละเอียดของชุดข้อมูล
4. จัดส่งหรือเชื่อมโยงชุดข้อมูลเปิดภาครัฐผ่านศูนย์กลางข้อมูลเปิดภาครัฐ (Data.go.th) ตามประเภทรูปแบบ และมาตรฐานของข้อมูลที่เปิดเผยแก่ประชาชน ตามที่สำนักงานพัฒนา รัฐบาลดิจิทัลกำหนด ทั้งนี้ ก่อนการเปิดเผยข้อมูลเปิดภาครัฐ ต้องได้รับอนุมัติจากหัวหน้าหน่วยงานของรัฐ
5. ให้หน่วยงานของรัฐและผู้ใช้ข้อมูลต้องปฏิบัติตามข้อกำหนด ข้อตกลง หรือเงื่อนไขการให้บริการและการใช้ข้อมูลของศูนย์กลางข้อมูลเปิดภาครัฐตามที่สำนักงานพัฒนารัฐบาลดิจิทัลกำหนด

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• จัดทำข้อมูลให้เป็นดิจิทัล (Digitalize Data) โดยกำหนดรูปแบบข้อมูลให้เป็นไปตามมาตรฐานที่กำหนด รวมถึงการจัดทำคำอธิบายชุดข้อมูลนั้นๆ เพื่อให้ผู้ใช้ข้อมูลสามารถเข้าใจเกี่ยวกับบริบทของข้อมูล	
	• จัดทำชุดข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ และเผยแพร่ข้อมูลเปิดภาครัฐบนศูนย์กลางข้อมูลเปิดภาครัฐ(https://data.go.th/) ตามรายชื่อชุดข้อมูลที่หน่วยงานสามารถเปิดเผยได้	

ด้านที่ 5 การสร้างความเชื่อมั่นต่อระบบการให้บริการภาครัฐว่าปลอดภัยจากภัยคุกคามทางไซเบอร์

การดำเนินงาน สขญ. มีการให้บริการระบบทั้งภายในและภายนอกหน่วยงาน รวมไปถึงภารกิจที่ สขญ. สนับสนุนในการพัฒนาระบบ และการบูรณาการข้อมูล ซึ่งมีข้อมูลจำนวนมากที่เกี่ยวข้องในการดำเนินงาน ซึ่งจะต้องได้รับการปกป้องให้เกิดความมั่นคงปลอดภัย ให้ผู้ใช้งานเกิดความเชื่อมั่นในการใช้บริการ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เป็นเรื่องสำคัญมากในปัจจุบัน เนื่องจากหน่วยงานมีการประยุกต์ใช้ระบบและบริการดิจิทัลในการทำงาน และภัยออนไลน์ทวีความรุนแรงมากขึ้นอย่างก้าวกระโดด ซึ่งหน่วยงานจำเป็นต้องป้องกันและรักษาข้อมูลที่สำคัญและความเชื่อมั่นในระบบดิจิทัลจากผู้ไม่ประสงค์ดี Cyber Threats) ซึ่งอาจมีเป้าหมายในการโจมตีหรือขโมยข้อมูลโดยดำเนินการ ดังนี้

1. ทบทวนปรับปรุงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นปัจจุบัน สามารถใช้ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการ อยู่ ในระดับที่ยอมรับได้ ทั้งนี้ นโยบายและแนวปฏิบัติดังกล่าว ควรครอบคลุมถึงประเด็นสำคัญ ดังนี้
   - การรักษาความลับ (Confidentiality) คือ มีการรับรองว่าข้อมูลที่จัดเก็บจะได้รับการคุ้มครองไว้เป็นความลับ ผู้มีสิทธิเท่านั้นที่จะเข้าถึงข้อมูลนั้นได้ และไม่ถูกเปิดเผยสู่บุคคลหรือหน่วยงานอื่นที่ไม่มีสิทธิ
   - การรักษาความสมบูรณ(Integrity) คือ มีการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา ข้อมูลจะคงอยู่อย่างถูกต้องและสมบูรณในทุกขั้นตอน
   - การพร้อมใช้(Availability) คือ มีการรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้
   - การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือ มีวิธีการสื่อสารที่แสดงข้อความแจ้งผู้ส่งข้อมูลเป็นหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้รับและผู้ส่งจะไม่สามารถปฏิเสธได้วาไม่มีความเกี่ยวของกับข้อมูลดังกล่าวในภายหลัง
2. ทบทวนปรับปรุงแผนตรวจสอบและประเมินความเสี่ยงด้าน Cyber Security เพื่อให้หน่วยงานมีความปลอดภัยจากการโจมตีทางไซเบอร์ ให้เป็นปัจจุบัน สามารถป้องกันข้อมูลสำคัญและรักษาความเชื่อมั่นของผู้ใช้งานรวมถึงลดความเสี่ยงให้ต่ำที่สุดเท่าที่เป็นไปได้ในการเกิดเหตุการณ์ Cyber Security ที่มีผลกระทบต่อองค์กรและกลุ่มลูกค้าของคุณโดยแผนควรระบุความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้นในระบบของหน่วยงาน, การวัดระดับความเสี่ยงและความถี่ที่อาจเกิดขึ้น, บุคคลหรือกลุ่มบุคคลที่มีความเสี่ยงด้านCyber Security, แผนการจัดการความเสี่ยงและมาตรการความปลอดภัยเพื่อลดความเสี่ยงและความรุนแรงของความเสี่ยง, และการตรวจสอบความปลอดภัยอย่างสม่ำเสมอเพื่อรักษาความเสถียรของระบบสารสนเทศ
3. ทบทวนปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response Plan) ซึ่งเป็นแผนการจัดการและรับมือกับเหตุการณ์ปัญหาทางความปลอดภัยทางไซเบอร์ในหน่วยงาน ทั้งนี้แผนการรับมือภัยคุกคามทางไซเบอร์ควรครอบคลุมถึงขั้นตอนต่างๆ ดังนี้
   - การเตรียมความพร้อม (Preparation) เช่น การกำหนดนโยบายและแนวทางปฏิบัติด้านความปลอดภัยทางไซเบอร์ การฝึกอบรมพนักงาน การประเมินความเสี่ยง

- การตรวจจับและวิเคราะห์ (Detection & Analysis) เช่น การติดตั้งระบบตรวจจับภัยคุกคาม การตรวจสอบความผิดปกติของเครือข่าย
- การตอบสนอง (Response) เช่น การแจ้งเตือนผู้ที่เกี่ยวข้อง การยับยั้งการโจมตี การกู้คืนระบบ
- การสอบสวนและฟื้นฟู (Investigation & Recovery) เช่น การระบุสาเหตุของการโจมตี การกู้คืนข้อมูลและระบบ

4. ทบทวนปรับปรุง ระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ให้มีประสิทธิภาพและทันสมัย โดยหน่วยงานควรจัดให้มีระบบ Cyber Security และมาตรการเพื่อป้องกันภัยคุกคามทางไซเบอร์ อย่างน้อยดังนี้
   - ระบบรักษาความปลอดภัยFirewall: ช่วยควบคุมการเข้าถึงและออกจากระบบขององค์กรและป้องกันการโจมตีจากภายนอก
   - โปรแกรมAnti-Virus/Anti-Malware: ช่วยตรวจจับและป้องกันไวรัสและโปรแกรมมัลแวร์ที่อาจเข้าสู่ระบบขององค์กร
   - ระบบยืนยันตัวตน (Authentication) และความปลอดภัยในการเข้าถึง(Access Control): เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
   - ระบบตรวจจับและระบบการตอบสนอง (Intrusion Detection and Response): เพื่อตรวจสอบและตอบสนองต่อพฤติกรรมที่ไม่ปกติในระบบ
   - การเข้ารหัสข้อมูล (Encryption): การเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายหรือเก็บข้อมูลเพื่อป้องกันการอ่านหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
   - การสำรองข้อมูล (Backup): การสำรองข้อมูลเพื่อรักษาข้อมูลสำคัญและระบบในกรณีเกิดภัยคุกคามหรือข้อผิดพลาด

ทั้งนี้ หน่วยงานควรดำเนินการทดสอบ Vulnerability Assessment Test (VA Test – การทดสอบตรวจหาช่องโหว่และข้อบกพร่องในระบบดิจิทัลขององค์กร โดยสำรวจและวิเคราะห์เพื่อระบุข้อบกพร่องที่มีภายในระบบ)และ Penetration Test (Pen Test – การจำลองการโจมตีจริงโดยผู้ทดสอบที่มีความเชี่ยวชาญด้าน Cyber Security เช่น การเจาะระบบเพื่อเข้าถึงข้อมูล) เป็นระยะตามความเหมาะสม เพื่อตรวจหาช่องโหว่และข้อบกพร่องความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน สำหรับการใช้บริการ Cloud ควรเลือกผู้ให้บริการที่มีมาตรฐานสากลด้าน Cyber Security เช่น ISO 20000 / ISO 27001 / CSA Star

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• ทบทวนปรับปรุงนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ให้มีความทันสมัย	
	• ทบทวนปรับปรุงแผนตรวจสอบและประเมินความเสี่ยงด้าน Cyber Security และมีการตรวจสอบความปลอดภัยอย่างสม่ำเสมอเพื่อรักษาความเสถียรของระบบสารสนเทศ	
	• ทบทวนปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response Plan) และมีการทดสอบ Execute ทดสอบแผนจำลองการเกิดเหตุภัยคุกคาม	
	• ทบทวนปรับปรุงระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ให้มีประสิทธิภาพ อย่างต่อเนื่อง เช่น Firewall , Anti-Virus ม ระบบยืนยันตัวตน ระบบ Access Control , Intrusion Detection and Response	
	• ทบทวนปรับปรุงการเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายหรือเก็บข้อมูลเพื่อป้องกันการอ่านหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาตมีการสำรองข้อมูลเพื่อรักษาข้อมูลสำคัญและระบบในกรณีเกิดภัยคุกคามหรือข้อผิดพลาด ให้มีความทันสมัยที่เพียงพอ	
	• ดำเนินการประเมินความเสี่ยงและตรวจสอบช่องโหว่ของระบบโครงสร้างพื้นฐาน และระบบบริการดิจิทัลเป็นประจำทุกปี	
	• จัดหาระบบเฝ้าระวังให้ครอบคลุมการป้องกันเชิงรุก และการแจ้งเตือน ในการรับมือภัยคุกคามในรูปแบบต่างๆ ที่มีประสิทธิภาพ เช่น จัดหาบริการศูนย์เฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ	
	• มีแผน BCP เพื่อให้ระบบที่สำคัญสามารถให้บริการได้อย่างต่อเนื่อง และมีการทดสอบประจำปี	• ทดสอบ BCP ระบบที่สำคัญที่ต้องสามารถให้บริการต่อเนื่องได้ประจำปี
	• มีการส่งเจ้าหน้าที่ไปอบรมเพื่อเพิ่มความสามารถในการออกแบบและปกป้องระบบได้	
	• ศึกษาภัยคุกคามใหม่และปรับปรุง เครื่องมือ เพื่อให้สามารถป้องกันระบบได้	
	• ทบทวนการสำรองข้อมูลเพื่อรักษาข้อมูลสำคัญและระบบในกรณีเกิดภัยคุกคามหรือข้อผิดพลาด	
	• ดำเนินการทดสอบ VA Test	• ดำเนินการทดสอบ VA Test และ การจำลองการโจมตีจริงโดยผู้ทดสอบที่มีความเชี่ยวชาญด้าน Cyber Security (Penetration Test)

ด้านที่ 6 การส่งเสริมศักยภาพและวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่บุคลากรภาครัฐ

ด้วย สขญ. เป็นหน่วยงานหลักที่มีหน้าที่ขับเคลื่อนประเทศด้วยข้อมูลขนาดใหญ่ มุ่งเน้นการส่งเสริมประสาน ให้คำปรึกษาและให้บริการแก่หน่วยงานของรัฐและเอกชน เพื่อเกิดการใช้ประโยชน์จากข้อมูลขนาดใหญ่ เพิ่มศักยภาพการบูรณาการ ยกระดับเศรษฐกิจและสังคมของประเทศ ดังนั้น สิ่งสำคัญคือการเตรียมความพร้อมของบุคลากรด้านเทคโนโลยีดิจิทัล เพื่อให้บุคลากรของ สขญ. สามารถปฏิบัติงานและขับเคลื่อนพันธกิจของสถาบันได้ตามวิสัยทัศน์ที่วางไว้ “Enabling Data-Driven Nation” โดย สขญ. มีแนวทางการส่งเสริมศักยภาพบุคลากรด้วยการยกระดับทักษะด้านดิจิทัลให้ครอบคลุม และสนับสนุนให้เกิดผู้นำด้านดิจิทัลในองค์กร รวมถึงสร้างวัฒนธรรมองค์กรที่ส่งเสริมให้เจ้าหน้าที่มีทัศนคติด้านดิจิทัลที่ดี และจัดกิจกรรมเพื่อส่งเสริมการสร้างสรรค์ไอเดียและนวัตกรรม โดยมีแนวทางการดำเนินการ ดังต่อไปนี้

1. สำรวจความต้องการและการวางแผนการอบรม : ทำการสำรวจเพื่อประเมินความต้องการและระดับความรู้ด้านเทคโนโลยีดิจิทัลของบุคลากร และจัดทำแผนการฝึกอบรมที่เหมาะสม
2. การฝึกอบรมและพัฒนา : จัดการฝึกอบรมทั้งรูปแบบ onsite และ online ในหัวข้อต่างๆ ที่สอดคล้องกับทักษะด้านดิจิทัลของบุคลากรภาครัฐทั้ง 7 ด้าน ได้แก่
    (1) ความสามารถด้านความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy)
    (2) ความสามารถด้านการปฏิบัติตามและ ใช้กฎหมายด้านดิจิทัล (Digital Governance)
    (3) ความสามารถด้านความเป็นผู้นำด้านดิจิทัล (Digital Leadership)
    (4) ความสามารถด้านการออกแบบกระบวนการและการให้บริการด้วยระบบดิจิทัลเพื่อการพัฒนาคุณภาพงานการประยุกต์ใช้เทคโนโลยี เพื่อการพัฒนางาน (Digital Technology)
    (5) ความสามารถด้านการพัฒนานวัตกรรม เพื่อการบริการ (Digital Service)
    (6) ความสามารถด้านการใช้ประโยชน์และ การใช้ข้อมูลร่วมกัน (Data Utilization and Sharing)
    (7) ความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)
3. การส่งเสริมวัฒนธรรมการใช้เทคโนโลยี : การสร้างความตระหนักรู้เกี่ยวกับประโยชน์ของการใช้เทคโนโลยีดิจิทัลผ่านการจัดกิจกรรม และส่งเสริมให้ผู้บริหารเป็นตัวอย่างในการใช้เทคโนโลยีและสนับสนุนการเปลี่ยนแปลงทางดิจิทัล
4. การประเมินผลและการปรับปรุง : ทำการประเมินผลการฝึกอบรมเพื่อวัดผลสำเร็จและหาจุดที่ต้องปรับปรุงอย่างต่อเนื่องตามผลการประเมินและข้อเสนอแนะจากบุคลากร

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• ดำเนินการจัดฝึกอบรมทั้งรูปแบบ onsite และ online ในหัวข้อที่สอดคล้องกับทักษะด้านดิจิทัลของบุคลากรภาครัฐทั้ง 7 ด้าน โดยสามารถดำเนินการจัดฝึกอบรมได้ร้อยละ 90 ของแผน รวมทั้งสร้างความตระหนักรู้เกี่ยวกับประโยชน์ของการใช้เทคโนโลยีดิจิทัลผ่านการจัดกิจกรรม และส่งเสริมให้ผู้บริหารเป็นตัวอย่างในการใช้เทคโนโลยีและสนับสนุนการเปลี่ยนแปลงทางดิจิทัล	• ดำเนินการจัดฝึกอบรมทั้งรูปแบบ onsite และ online ในหัวข้อที่สอดคล้องกับทักษะด้านดิจิทัลของบุคลากรภาครัฐทั้ง 7 ด้าน โดยสามารถดำเนินการจัดฝึกอบรมได้ร้อยละ 100 ของแผน พร้อมทั้งนำผลการประเมินการฝึกอบรมในปีที่ผ่านๆ มาวิเคราะห์ เพื่อปรับปรุงแนวทางการส่งเสริมศักยภาพและวัฒนธรรมการใช้เทคโนโลยีดิจิทัลแก่บุคลากร เพื่อยกระดับศักยภาพและความพร้อมในการขับเคลื่อนรัฐบาลดิจิทัลได้จริง

ด้านที่ 7 การทบทวน ปรับปรุง พัฒนากฎหมาย หรือ กฎระเบียบ มาตรการที่เอื้อต่อการพัฒนารัฐบาลดิจิทัล

ด้วยสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) เป็นองค์การมหาชนภายใต้การกำกับของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตามพระราชกฤษฎีกาจัดตั้งสถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) พ.ศ. ๒๕๖๖ ซึ่งประกาศในราชกิจจานุเบกษาเมื่อวันที่ ๒ มิถุนายน ๒๕๖๖ สถาบันเป็นหน่วยงานหลักที่มีหน้าที่ขับเคลื่อนประเทศด้วยข้อมูลขนาดใหญ่ มุ่งเน้นการส่งเสริม ประสาน ให้คำปรึกษาและให้บริการแก่หน่วยงานของรัฐและเอกชน เพื่อเกิดการใช้ประโยชน์จากข้อมูลขนาดใหญ่ เพิ่มศักยภาพการบูรณาการยกระดับเศรษฐกิจและสังคมของประเทศ โดยมุ่งเน้นการพัฒนารูปแบบและแนวทางการดำเนินงาน ๓ แนวทาง คือ การส่งเสริม สนับสนุน และให้บริการ เพื่อให้เกิดการใช้ประโยชน์ข้อมูลขนาดใหญ่ การพัฒนาระบบนิเวศน์ในห่วงโซ่คุณค่าด้านข้อมูลและศักยภาพของผู้ประกอบการในประเทศและการเสริมสร้างขีดความสามารถของบุคลากรด้านข้อมูลขนาดใหญ่ของประเทศ

โดยการดำเนินงาน ตามภารกิจของหน่วยงานที่เป็นการศึกษากฎหมาย กฎระเบียบ มาตรการต่างๆ จะสอดคล้องกับการดำเนินงานของหน่วยงานและตอบสนองต่อการผลักดันรัฐบาลดิจิทัล เช่น การจัดทำประกาศ ในเรื่อง นโยบายธรรมาภิบาลข้อมูล เพื่อให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐ ผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และประกาศ เรื่อง ช่องทางอิเล็กทรอนิกส์สำหรับการติดต่อสถาบันข้อมูล ขนาดใหญ่ พ.ศ. ๒๕๖๗ เพื่อให้สอดคล้องกับพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ เป็นต้น

ทั้งนี้ สขญ. จะมีการรวบรวมประเด็นปัญหา อุปสรรคต่างๆ ที่เกิดขึ้น พร้อมทบทวนกฎหมาย กฎระเบียบ และมาตรการ ทั้งนี้ หากพบว่ามีการดำเนินการที่ไม่สอดคล้องกับแนวทางตามภารกิจในอนาคตที่เอื้อต่อการเป็นรัฐบาลดิจิทัลได้ จะมีการพิจารณาทบทวนและปรับปรุงกฎหมายกฎระเบียบ และมาตรการ

ประกอบกับพิจารณาปรับปรุงโครงสร้างส่วนงานให้สอดคล้องกับบริบทปัจจุบันหรือพัฒนากฎระเบียบใหม่ที่เกี่ยวข้องกับสถาบันให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไป และสร้างความตระหนักรู้ให้กับบุคลากรของหน่วยงานให้มีความเข้าใจกับบริบทของกฎหมาย ซึ่งจะทำให้การบริหารงานและการให้บริการ ทางดิจิทัลมีประสิทธิภาพมากขึ้น

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• ทบทวนและศึกษากฎหมาย หรือกฎระเบียบ มาตรการที่เอื้อต่อการพัฒนารัฐบาลดิจิทัล	• ทบทวนและศึกษากฎหมาย หรือกฎระเบียบ มาตรการที่เอื้อต่อการพัฒนารัฐบาลดิจิทัล

ด้านที่ 8 การส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนในการพัฒนารัฐบาลดิจิทัล

ในการดำเนินงาน สขญ. โดยโครงการพัฒนาอุตสาหกรรมและประสานเครือข่ายด้านข้อมูลขนาดใหญ่ มีหน้าที่พัฒนาผู้ประกอบการโดยสร้างทั้งอุปสงค์และอุปทานของศาสตร์ด้านข้อมูลในประเทศ เพื่อสร้างความเข้าใจจากการใช้ประโยชน์ข้อมูลเชิงวิเคราะห์ควบคู่กับการพัฒนาอุตสาหกรรม และสร้างการรับรู้ด้านธุรกิจที่เกี่ยวกับการใช้ข้อมูลและปัญญาประดิษฐ์ ซึ่งรูปแบบการทำงาน จะสร้างกลไกที่สามารถสนับสนุนให้เกิดระบบนิเวศของอุตสาหกรรมข้อมูลขนาดใหญ่ ผ่านการแบ่งปันความรู้ ทรัพยากร และความเชี่ยวชาญ โดยการสร้างความร่วมมือระหว่างภาครัฐและเอกชนที่เป็นผู้เล่นในมิติต่างๆ ประกอบด้วย องค์กรผู้ใช้ข้อมูล ผู้ผลิตข้อมูล บริษัทหรือบุคคลด้านการบูรณาการและวิเคราะห์ข้อมูล ผู้วางระเบียบ (Regulator) ผู้ผลิตเทคโนโลยี ฯลฯ

ทั้งนี้ จึงได้มีการพัฒนาแพลตฟอร์มข้อมูล Ecosystem ที่จัดเก็บทะเบียนข้อมูลผู้ประกอบการในธุรกิจข้อมูลขนาดใหญ่ของประเทศ การรวบรวมข้อมูลงานสัมมนา กิจกรรม และเครือข่ายความร่วมมือจากทุกภาคส่วน ไม่ว่าจะเป็น ผู้ประกอบการ นักวิจัย หน่วยงานภาครัฐ หน่วยงานภาคเอกชน และประชาชน มีวัตถุประสงค์เพื่อสนับสนุนการจับคู่ธุรกิจและให้บริการด้านเทคโนโลยีข้อมูลขนาดใหญ่และปัญญาประดิษฐ์ (Big Data & AI) ซึ่งเป็นการสร้างเครือข่ายและกลไกให้กับผู้เล่นในระบบนิเวศ Big Data & AI เช่น การเชื่อมโยงพันธมิตรจากรัฐ เอกชน สถาบันการศึกษา รวมถึงส่งเสริมการแลกเปลี่ยนองค์ความรู้ระหว่างภาคส่วนต่าง ๆ เพื่อก่อให้เกิดความร่วมมือเชิงเศรษฐกิจและนวัตกรรมอย่างยั่งยืนให้เกิดการเติบโตของอุตสาหกรรมข้อมูลและปัญญาประดิษฐ์ในประเทศไทย

ทั้งนี้ ข้อมูลต่างๆ ที่อยู่ในแพลตฟอร์มจะมีการจัดเก็บอย่างมีประสิทธิภาพเพื่อให้สามารถสืบค้นและนำข้อมูลมาใช้ให้เกิดประโยชน์ได้ ทำให้ต้องมีการศึกษาข้อมูลที่สอดคล้องกับกฎระเบียบ มาตรการต่างๆ เช่น ข้อมูลส่วนบุคคล แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570

ปีงบประมาณ	ปี 2569	ปี 2570
เป้าหมาย	• ปรับปรุงแพลตฟอร์มเพื่อให้รับรองการสนับสนุนทุนให้แก่ผู้ประกอบการ และการให้ทุนสนับสนุนองค์กรเพื่อพัฒนาบุคคลธรรมดา ในการพัฒนาองค์	• ปรับปรุงแพลตฟอร์มเพื่อเพิ่มประสิทธิภาพในการส่งเสริมจับคู่ธุรกิจ และให้บริการข้อมูลผู้ประกอบการ

ปีงบประมาณ	ปี 2569	ปี 2570
	ความรู้ด้านการวิเคราะห์ข้อมูลขนาดใหญ่และเทคโนโลยีที่เกี่ยวข้อง • ระบบฐานข้อมูลผู้ประกอบการ/เครือข่ายด้านเทคโนโลยีข้อมูลขนาดใหญ่ และปัญญาประดิษฐ์ที่ได้รับการปรับปรุง	