

แผนแม่บทมหาวิทยาลัยดิจิทัล

มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์

ผู้ช่วยศาสตราจารย์ ดร.เศรษฐพงศ์ วงษ์อินทร์

หมายเลข	ความหมาย	วันที่	โดย
V0.1	เริ่มเอกสาร	1 พฤษภาคม 2568	ผศ.ดร.เศรษฐพงศ์ วงษ์อินทร์
V0.2	เพิ่ม กรอบการทำงาน	16 พฤษภาคม 2568	ผศ.ดร.เศรษฐพงศ์ วงษ์อินทร์
V0.3	เพิ่ม ร่าง KPI, รหัสเอกสารแต่ละองค์ประกอบ	13 มิถุนายน 2568	ผศ.ดร.เศรษฐพงศ์ วงษ์อินทร์
V0.4	เพิ่มโครงสร้างคณะกรรมการมหาวิทยาลัยดิจิทัล	1 กรกฎาคม 2568	ผศ.ดร.เศรษฐพงศ์ วงษ์อินทร์



บทสรุปผู้บริหาร (Executive Summary)

ในช่วงทศวรรษที่ผ่านมา โลกได้ก้าวเข้าสู่ยุคของการเปลี่ยนผ่านอย่างรวดเร็วภายใต้กระแส ดิจิทัลทรานส์ฟอร์เมชัน (Digital Transformation) ซึ่งไม่เพียงส่งผลต่อภาคธุรกิจเท่านั้น แต่ยังส่งผลต่อภาคการศึกษาทั่วโลก รวมถึงมหาวิทยาลัยในประเทศไทยอย่างหลีกเลี่ยงไม่ได้

สำหรับมหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ ซึ่งมีพันธกิจในการเป็นกลไกขับเคลื่อนสังคมฐานราก การพัฒนาสู่มหาวิทยาลัยดิจิทัล (Digital University) จึงไม่ใช่เรื่องทางเลือกอีกต่อไป แต่คือ เงื่อนไขของการอยู่รอด และ โอกาสในการยกระดับมหาวิทยาลัยทั้งระบบ ให้ทันสมัย ยืดหยุ่น และตอบโจทย์ผู้เรียน ผู้ปฏิบัติงาน และชุมชนอย่างแท้จริง

เพื่อรองรับการเปลี่ยนผ่านนี้ แผนแม่บทมหาวิทยาลัยดิจิทัลฉบับนี้ ได้รับการจัดทำขึ้นในลักษณะ พิมพ์เขียว สำหรับการพัฒนาและบริหารมหาวิทยาลัยในยุคใหม่อย่างรอบด้าน โดยมีแนวคิดหลัก 3 ประการ ได้แก่:

- 1) ยึดโยงกับนโยบายระดับชาติ เช่น นโยบายมหาวิทยาลัย 4.0 ของกระทรวง อว., แผนพัฒนารัฐบาลดิจิทัลของ DGA, PDPA และ NIST Cybersecurity Framework
- 2) กำหนดกรอบการพัฒนาที่ครอบคลุมทุกมิติ ภายใต้โครงสร้าง VRU Digital University Framework (V-DUF) ซึ่งแบ่งออกเป็น 8 องค์ประกอบ ได้แก่ การบริหารจัดการ, โครงสร้างพื้นฐาน, ระบบบริการ, บุคลากร, ข้อมูล, ความปลอดภัย, พันธมิตร และระบบติดตามผล
- 3) มีแผนปฏิบัติการที่ชัดเจน เริ่มต้นจากแผนระยะสั้น 6 เดือน พร้อมต่อยอดสู่แผน 3 ปี โดยกำหนดโครงการนำร่อง ตัวชี้วัดความสำเร็จ และกลไกการติดตามผลอย่างเป็นระบบ

ประโยชน์ที่ได้รับ

- 1) มหาวิทยาลัยจะมีระบบบริหารจัดการที่ทันสมัยขึ้น ลดการใช้เอกสาร เพิ่มความโปร่งใสและรวดเร็วในการให้บริการ เช่น การลงนามเอกสารผ่านระบบอิเล็กทรอนิกส์, การใช้งาน SSO, และ e-Service ที่นักศึกษาสามารถเข้าถึงได้ตลอด 24 ชั่วโมง
- 2) บุคลากรจะสามารถทำงานได้สะดวกและมีประสิทธิภาพสูงขึ้น ด้วยการใช้เครื่องมือดิจิทัล ช่วยลดภาระงานประจำ และสามารถพัฒนาทักษะใหม่ ๆ เช่น AI, Data Analytics ที่จะกลายเป็นพื้นฐานของการทำงานในอนาคต
- 3) นักศึกษาจะได้รับประสบการณ์การเรียนรู้ที่ดีขึ้น ทั้งในห้องเรียนดิจิทัล (Digital Classroom), ระบบ LMS ที่ยืดหยุ่น และการเข้าถึงบริการต่าง ๆ ผ่าน Mobile App และ Portal เดียว
- 4) ผู้บริหารสามารถเห็นภาพรวมขององค์กรผ่าน Dashboard และข้อมูลวิเคราะห์ที่แม่นยำ ช่วยให้ตัดสินใจได้อย่างมีข้อมูลรองรับ (data-driven)
- 5) มหาวิทยาลัยจะมีความพร้อมในการรองรับการประกันคุณภาพ การตรวจสอบจากหน่วยงานรัฐ และการขอรับรองมาตรฐานพัฒนาระบบดิจิทัลในอนาคต

หากไม่ดำเนินการ อะไรคือความเสี่ยง

- 1) ระบบภายในมหาวิทยาลัยจะยังคงพึ่งพากระบวนการแบบเดิมที่ล่าช้า เบื้องทรัพยากร และไม่ตอบโจทย์ความคาดหวังของผู้เรียนยุคใหม่
- 2) การขาดแคลนข้อมูลที่เชื่อมโยงกันจะส่งผลให้การบริหารงานไม่มีประสิทธิภาพ เสี่ยงต่อความผิดพลาดในการตัดสินใจ
- 3) บุคลากรขาดทักษะดิจิทัลที่จำเป็นต่อการทำงานในอนาคต ทำให้เกิด Digital Divide ภายในองค์กร
- 4) มหาวิทยาลัยจะตกอยู่ในความเสี่ยงจากภัยคุกคามทางไซเบอร์ และอาจละเมิดกฎหมาย PDPA โดยไม่รู้ตัว
- 5) การขาดความพร้อมเชิงดิจิทัลจะทำให้มหาวิทยาลัยเสียโอกาสในการขอรับการสนับสนุนจากรัฐหรือภาคเอกชน และไม่สามารถแข่งขันกับสถาบันอื่นที่พัฒนาไปไกลแล้ว

บทสรุป

แผนแม่บทฉบับนี้มีได้เป็นเพียงเอกสารเชิงนโยบาย หากแต่เป็นเครื่องมือในการ บริหารความเปลี่ยนแปลง ของมหาวิทยาลัยทั้งระบบ ที่จะช่วยลดจุดอ่อน เสริมจุดแข็ง และนำพาองค์กรสู่อนาคตอย่างมั่นคงและยั่งยืน

มหาวิทยาลัยจึงควร กล้าเริ่ม กล้าปรับ และกล้าขับเคลื่อน ด้วยพลังของดิจิทัล เพื่อให้ทันต่อยุคสมัย สอดคล้องกับพันธกิจของมหาวิทยาลัย และตอบสนองต่อความคาดหวังของสังคมอย่างแท้จริง



แผนแม่บทมหาวิทยาลัยดิจิทัล มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์

1. ที่มาของแนวคิด Digital University ในประเทศไทย

ในช่วงทศวรรษที่ผ่านมา สังคมไทยได้เผชิญกับการเปลี่ยนแปลงอย่างรวดเร็วจากกระแสดิจิทัลทรานส์ฟอร์เมชัน (Digital Transformation) ที่เข้ามามีบทบาทในแทบทุกภาคส่วนของประเทศ รวมถึงในระบบการอุดมศึกษา การพัฒนามหาวิทยาลัยให้เข้าสู่ยุคดิจิทัลจึงไม่ได้เป็นเพียงทางเลือก แต่กลายเป็นภารกิจจำเป็นในการปรับตัวเพื่อความอยู่รอด และการยกระดับศักยภาพสู่มาตรฐานใหม่ของโลกการศึกษา

1.1 บทบาทของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.)

กระทรวง อว. ในฐานะหน่วยงานหลักที่กำกับดูแลการอุดมศึกษา ได้กำหนดยุทธศาสตร์ มหาวิทยาลัย 4.0 เพื่อเป็นทิศทางการพัฒนาสถาบันอุดมศึกษาไทย โดยหนึ่งในประเด็นสำคัญคือการเปลี่ยนผ่านมหาวิทยาลัยไปสู่การเป็น Digital University

ใน แผนแม่บท อว. ระยะ 20 ปี และ แผนพัฒนาอุดมศึกษาล่าสุด (พ.ศ. 2566–2570) ได้ระบุอย่างชัดเจนว่า มหาวิทยาลัยควรประยุกต์ใช้เทคโนโลยีดิจิทัลในการปรับปรุงระบบการเรียนรู้ การบริหารจัดการ และการให้บริการต่าง ๆ เพื่อสร้างความคล่องตัว โปร่งใส และมีประสิทธิภาพสูงสุด

1.2 บทบาทของสำนักงานพัฒนารัฐบาลดิจิทัล (DGA)

แม้ว่ามหาวิทยาลัยจะอยู่ภายใต้สังกัดของ อว. แต่ในฐานะหน่วยงานของรัฐ ก็ต้องปฏิบัติตามกรอบของรัฐบาลดิจิทัลเช่นกัน โดย สำนักงานรัฐบาลดิจิทัล (DGA) เป็นหน่วยงานที่กำหนดแนวนโยบาย Digital Government ซึ่งมหาวิทยาลัยต้องนำไปประยุกต์ใช้ โดยเฉพาะประเด็นสำคัญ ได้แก่

- 1) การให้บริการผ่านระบบ e-Service และ e-Document
- 2) การใช้ Cloud ภาครัฐ (Government Cloud)
- 3) การจัดการข้อมูลตามหลัก Data Governance
- 4) การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)
- 5) การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ในแผน Digital Government Plan 2566–2570 ยังระบุชัดว่าหน่วยงานภาครัฐทุกแห่ง รวมถึงสถาบันอุดมศึกษา ต้องมีแผนพัฒนาระบบดิจิทัลให้สอดคล้องกับแนวทางดังกล่าว

1.3 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) และหน่วยงานเครือข่าย

อีกหน่วยงานสำคัญที่ส่งผลต่อการพัฒนา Digital University คือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) ซึ่งผลักดันการปฏิรูประบบราชการผ่านแนวคิด Cloud First Policy และ Digital Transformation ภาครัฐ โดยเน้นให้หน่วยงานต่าง ๆ รวมถึงมหาวิทยาลัย ปรับเปลี่ยนสู่การใช้เทคโนโลยีคลาวด์ และระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบ

ขณะเดียวกัน สำนักงานคณะกรรมการการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ยังมีบทบาทในการสนับสนุนการจัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม โดยให้ความสำคัญกับโครงการ Smart Campus / Smart Education ซึ่งสอดคล้องกับแนวคิด Digital University อย่างเต็มรูปแบบ

2. Framework กลางในการพัฒนามหาวิทยาลัยดิจิทัล

การเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัล ไม่สามารถเกิดขึ้นได้จากความตั้งใจเพียงอย่างเดียว แต่ต้องอาศัยกรอบแนวทาง ที่ชัดเจนและครอบคลุม เพื่อให้การดำเนินการเป็นไปอย่างเป็นระบบ มีมาตรฐาน และสามารถเชื่อมโยงกับนโยบายระดับชาติและสากลได้อย่างมีประสิทธิภาพ

ในระดับประเทศ มีการกำหนดกรอบการทำงานหรือกรอบแนวทางกลางที่เกี่ยวข้องกับการพัฒนาหน่วยงานภาครัฐและการอุดมศึกษาไว้หลากหลาย โดยสามารถสรุปแนวทางสำคัญที่มหาวิทยาลัยควรใช้เป็นหลักอ้างอิงในการออกแบบแผนแม่บทได้ ดังนี้

2.1 กรอบ Digital Government ของ DGA

สำนักงานพัฒนารัฐบาลดิจิทัล (DGA) ได้จัดทำ กรอบ Digital Government เพื่อให้หน่วยงานของรัฐสามารถพัฒนาตนเองให้เป็นองค์กรที่ทันสมัย โปร่งใส และให้บริการประชาชนอย่างมีประสิทธิภาพ ซึ่งสามารถนำมาประยุกต์ใช้กับมหาวิทยาลัยได้อย่างดี โดยมีองค์ประกอบหลัก 5 ประการ ได้แก่:

Digital Service – พัฒนาการให้บริการแบบอิเล็กทรอนิกส์แก่ประชาชนหรือนักศึกษา

Open Data & Interoperability – การเปิดเผยข้อมูลเพื่อการใช้ประโยชน์ และการเชื่อมโยงข้อมูลระหว่างระบบ

Digital Workforce – การส่งเสริมและพัฒนาทักษะด้านดิจิทัลแก่บุคลากร

Data Governance – การบริหารจัดการข้อมูลภายในองค์กรอย่างมีมาตรฐาน

Cybersecurity & Privacy – การรักษาความปลอดภัยของระบบและการคุ้มครองข้อมูลส่วนบุคคล

DGA ยังสนับสนุนการใช้ระบบคลาวด์ภาครัฐ (G-Cloud), การประเมิน Digital Maturity และการพัฒนา Platform ภาครัฐร่วมกัน (Shared Services)

2.2 กรอบ มหาวิทยาลัย 4.0 ของกระทรวง อว.

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) ได้กำหนดกรอบการพัฒนา มหาวิทยาลัยในบริบทใหม่ภายใต้แนวคิด มหาวิทยาลัย 4.0 ซึ่งชี้ให้เห็นว่ามหาวิทยาลัยไม่ควรเป็นเพียงสถานที่ให้ความรู้ แต่ต้องกลายเป็นศูนย์กลางนวัตกรรม แหล่งผลิตกำลังคนแห่งอนาคต และมีการบริหารจัดการแบบยืดหยุ่นทันสมัย

สาระสำคัญของกรอบนี้ครอบคลุม 3 ด้านหลัก ได้แก่:

- 1) การเรียนรู้แบบยืดหยุ่น (Flexible Learning) รองรับการเรียนรู้ออนไลน์, Upskill/Reskill, และ Non-degree
- 2) การบริหารจัดการอิงข้อมูล (Data-driven Management) ส่งเสริมการใช้ Dashboard และ Big Data ในการตัดสินใจ
- 3) การเชื่อมโยงกับภาคเศรษฐกิจและชุมชน (University Engagement) มหาวิทยาลัยต้องเป็นกลไกพัฒนาเศรษฐกิจฐานรากผ่านนวัตกรรม

2.3 กรอบความมั่นคงปลอดภัยไซเบอร์ NIST CSF 2.0

สำหรับด้านความปลอดภัยทางไซเบอร์ ซึ่งเป็นหัวใจสำคัญของการดำเนินงานในโลกดิจิทัล มหาวิทยาลัยควรใช้ NIST Cybersecurity Framework (CSF) เวอร์ชัน 2.0 เป็นกรอบหลักในการบริหารความเสี่ยง ซึ่งแบ่งออกเป็น 6 ฟังก์ชันหลัก ได้แก่:

- 1) Govern – วางโครงสร้างการกำกับดูแลและนโยบายความปลอดภัย
- 2) Identify – ระบุความเสี่ยง ทรัพย์สิน และช่องโหว่
- 3) Protect – วางมาตรการควบคุมป้องกันภัยคุกคาม
- 4) Detect – ตรวจสอบเหตุการณ์ผิดปกติอย่างรวดเร็ว
- 5) Respond – ตอบสนองและแก้ไขเมื่อเกิดเหตุการณ์
- 6) Recover – ฟื้นฟูระบบและดำเนินการต่ออย่างมีประสิทธิภาพ

กรอบนี้ได้รับการยอมรับในระดับสากล และประเทศไทยก็นำไปใช้ในการกำกับหน่วยงานรัฐและรัฐวิสาหกิจ รวมถึงมหาวิทยาลัยที่มีระบบสารสนเทศขนาดใหญ่

ตารางที่ 1 กรอบการทำงานที่สอดคล้องกับ Digital University

กรอบการทำงาน	หน่วยงานต้นทาง	จุดเน้น
NIST CSF 2.0	National Institute of Standards and Technology (USA)	มาตรฐานการบริหารความมั่นคงปลอดภัยไซเบอร์ 6 ฟังก์ชัน (Govern-Recover)
DGA Digital Government Framework	สำนักงานรัฐบาลดิจิทัล (DGA)	บริการดิจิทัล, Open Data, Cloud, Data Governance
มหาวิทยาลัย 4.0 (อว.)	กระทรวง อว.	Flexible Learning, Data-driven Management, Engagement with Community
PDPA Compliance Framework	กระทรวงดิจิทัลฯ (ดีอีเอส)	การจัดการข้อมูลส่วนบุคคล, สิทธิของเจ้าของข้อมูล, การขอความยินยอม

ในการพัฒนาแผนแม่บท Digital University ของมหาวิทยาลัยวลัยลักษณ์ฯ (VRU) จึงจำเป็นต้องบูรณาการทั้ง 3 กรอบการทำงานเข้าด้วยกัน เพื่อให้สามารถตอบสนองต่อทั้งนโยบายระดับประเทศ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย และมาตรฐานสากลอย่างรอบด้าน

3.ระเบียบ/กฎหมาย ที่เกี่ยวข้อง

การพัฒนามหาวิทยาลัยดิจิทัลในบริบทของประเทศไทย ไม่สามารถดำเนินการได้อย่างอิสระโดยปราศจากกรอบกำกับที่ชัดเจน ทั้งในเชิงนโยบาย กฎหมาย และข้อบังคับต่าง ๆ ที่เกี่ยวข้องโดยตรงกับการเปลี่ยนผ่านสู่ระบบดิจิทัล โดยเฉพาะเมื่อมหาวิทยาลัยถือเป็นหน่วยงานของรัฐ ที่ต้องดำเนินการภายใต้กรอบของรัฐธรรมนูญ แผนยุทธศาสตร์ชาติ และกฎหมายเฉพาะทางต่าง ๆ

ในหัวข้อนี้ จะได้นำเสนอ กฎหมายและระเบียบที่สำคัญ ซึ่งมีผลกระทบและเกี่ยวข้องกับการวางระบบมหาวิทยาลัยดิจิทัลโดยตรง เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้อง โปร่งใส และสามารถตรวจสอบได้

3.1 พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

กฎหมายฉบับนี้มีผลบังคับใช้อย่างเป็นทางการตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 โดยมีเป้าหมายเพื่อกำกับดูแลการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างเป็นธรรม ปลอดภัย และเคารพสิทธิของเจ้าของข้อมูล

สำหรับมหาวิทยาลัย การดำเนินงานในหลายมิติ เช่น การรับสมัครนักศึกษา การเก็บข้อมูลผลการเรียน หรือแม้แต่การถ่ายภาพกิจกรรม ล้วนแล้วแต่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งสิ้น ดังนั้น การพัฒนาแพลตฟอร์มและระบบดิจิทัลภายในองค์กรจึงต้องออกแบบให้ สอดคล้องกับ PDPA อย่างเคร่งครัด ได้แก่

- 1) การตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- 2) การขอความยินยอมก่อนเก็บข้อมูล (Consent)
- 3) การจัดเก็บข้อมูลตามหลัก Data Minimization
- 4) การจัดทำระบบสิทธิของเจ้าของข้อมูล เช่น การขอลบหรือเข้าถึงข้อมูล

3.2 พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กฎหมายฉบับนี้เป็นอีกหนึ่งเสาหลักที่กำหนดให้หน่วยงานรัฐ ซึ่งรวมถึงมหาวิทยาลัย ต้องมีมาตรการในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีระบบและเป็นรูปธรรม มหาวิทยาลัยต้อง:

- 1) จัดตั้งทีมเฝ้าระวังและตอบสนองเหตุการณ์ไซเบอร์ (CSIRT)
- 2) จัดทำแผนความมั่นคงปลอดภัยไซเบอร์
- 3) รายงานเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อระบบสารสนเทศภายในระยะเวลาอันสั้น
- 4) ใช้แนวทางมาตรฐานสากล เช่น NIST CSF 2.0 ในการวางระบบ

การไม่ปฏิบัติตามอาจส่งผลให้ข้อมูลสำคัญ เช่น ระบบทะเบียนนักศึกษา, ระบบเงินเดือน หรือฐานข้อมูลงานวิจัย ตกอยู่ในความเสี่ยงที่รุนแรง

3.3 ระเบียบและมาตรฐานจากหน่วยงานภาครัฐ

นอกจากกฎหมายข้างต้น ยังมีระเบียบและแนวปฏิบัติจากหน่วยงานกลางที่มหาวิทยาลัยต้องนำไปใช้หรือยึดเป็นแนวทาง ได้แก่:

- 1) มาตรฐานการพัฒนาระบบราชการดิจิทัล (Digital Government Standard)
- 2) ออกโดย สำนักงานรัฐบาลดิจิทัล (DGA) ซึ่งระบุองค์ประกอบ เช่น e-Service, Open Data, Digital Identity, Data Governance
- 3) Cloud First Policy
- 4) แนวทางที่ส่งเสริมให้หน่วยงานรัฐใช้ระบบคลาวด์ภาครัฐ (G-Cloud) เพื่อความคุ้มค่าและความปลอดภัยในการจัดเก็บและประมวลผลข้อมูล
- 5) แนวทางจัดซื้อจัดจ้างระบบ IT และ Software License
- 6) โดยสำนักงานงบประมาณ/กรมบัญชีกลาง ซึ่งระบุถึงประเภทของระบบที่สามารถจัดซื้อได้ วิธีการคำนวณมูลค่าระบบ และข้อจำกัดที่ควรพึงระวัง

ตารางที่ 2 แสดงกฎหมายหลัก

ชื่อกฎหมาย	ประเด็นสำคัญ	สิ่งที่มหาวิทยาลัยต้องดำเนินการ
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)	การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอม และมี การจัดการข้อมูลอย่างปลอดภัย	- แต่งตั้ง DPO (เจ้าหน้าที่คุ้มครองข้อมูล) - ขอ Consent จากผู้ใช้บริการ - สร้างระบบแจ้งสิทธิของเจ้าของข้อมูล - จัดอบรม PDPA ให้บุคลากร

พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562	หน่วยงานรัฐต้องมีระบบป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์	- ตั้ง CSIRT (ทีมตอบสนองภัยไซเบอร์) - ทำแผนความปลอดภัยระบบสารสนเทศ - รายงานเหตุการณ์ผิดปกติ - ปฏิบัติตามแนวทาง NIST CSF 2.0
พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	เอกสารและลายเซ็นอิเล็กทรอนิกส์มีผลทางกฎหมายเท่ากับเอกสารกระดาษ	- ใช้ e-Document ในการดำเนินงาน - วางระบบจัดเก็บ/ตรวจสอบลายเซ็นดิจิทัล - ปรับกระบวนการให้สอดคล้องกับระบบอิเล็กทรอนิกส์
พ.ร.บ. การศึกษาแห่งชาติ (ฉบับใหม่)	ส่งเสริมการเรียนรู้ตลอดชีวิต การเรียนแบบยืดหยุ่น และการประเมินผลหลายรูปแบบ	- พัฒนาแพลตฟอร์ม e-Learning และ Non-degree - ปรับหลักสูตรรองรับ Upskill/Reskill - ส่งเสริมการเรียนรู้ผ่านระบบดิจิทัล

3.4 กฎหมายอื่นที่เกี่ยวข้อง

แม้ว่าพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเป็นกฎหมายหลักที่เกี่ยวข้องโดยตรงกับการพัฒนาเทคโนโลยีดิจิทัลในภาครัฐและมหาวิทยาลัย แต่ในความเป็นจริง ยังมีกฎหมายอื่น ๆ อีกหลายฉบับที่แวดล้อม และมีผลต่อการดำเนินงานในฐานะหน่วยงานภาครัฐ โดยเฉพาะอย่างยิ่งในกระบวนการจัดการศึกษา การจัดซื้อจัดจ้าง การใช้เอกสารอิเล็กทรอนิกส์ หรือแม้แต่ว่าการกำหนดโครงสร้างบุคลากรดิจิทัลภายในมหาวิทยาลัย

กฎหมายเหล่านี้อาจไม่ได้กล่าวถึงดิจิทัลโดยตรงไปตรงมาในชื่อเรื่อง แต่กลับส่งผลกระทบมีนัยยะสำคัญต่อความถูกต้องตามระเบียบ และความคล่องตัวในการบริหารจัดการของมหาวิทยาลัย หากสามารถอ่านเกม และเชื่อมโยงกับแนวทางพัฒนา Digital University ได้อย่างเข้าใจ ก็จะช่วยลดข้อจำกัด และเปิดโอกาสให้กับ การขับเคลื่อนนวัตกรรมภายในมหาวิทยาลัยได้อย่างยั่งยืน

ตารางที่ 3 แสดงกฎหมายอื่น ๆ ที่เกี่ยวข้อง

กฎหมาย/ระเบียบ	ความเกี่ยวข้อง
พ.ร.บ. การศึกษาแห่งชาติ (ฉบับใหม่)	เปิดกว้างให้มหาวิทยาลัยจัดการศึกษาแบบดิจิทัล / Online / Non-degree
พ.ร.บ. อิเล็กทรอนิกส์ พ.ศ. 2544	รองรับการใช้เอกสารอิเล็กทรอนิกส์, ลายมือชื่อดิจิทัล ฯลฯ
ระเบียบ ก.พ.อ. / ก.พ.ร.	ใช้ในการจัดโครงสร้างตำแหน่ง, บุคลากรที่เกี่ยวข้องกับ Digital Transformation
ระเบียบ มหาวิทยาลัย	เช่น ประกาศเรื่องการใช้งาน IT, การอนุญาตเข้าถึงระบบ ฯลฯ (อาจต้องปรับปรุงใหม่)

4. สรุปแนวทางที่ควร ทำตาม หรือ อิงอ้าง

จากการวิเคราะห์นโยบายระดับชาติ กฎหมายที่เกี่ยวข้อง และกรอบการทำงานกลางที่หน่วยงานรัฐและอุดมศึกษาใช้เป็นแนวทางในการพัฒนาดิจิทัล จะเห็นได้ว่าการพัฒนามหาวิทยาลัยดิจิทัล ไม่ได้เป็นเรื่อง

ใหม่หรือแยกขาดจากระบบราชการไทย แต่เป็นกลยุทธ์ร่วมระดับประเทศ ที่มีหน่วยงานกำกับอย่างชัดเจน ทั้งในมิตินโยบาย กฎหมาย และเทคโนโลยี

ในการดำเนินแผนแม่บท Digital University อย่างมีประสิทธิภาพ มหาวิทยาลัยจึงควรอิงอ้างอิงและดำเนินการตามแนวทางหลัก 3 กลุ่มต่อไปนี้:

4.1 แนวนโยบายระดับชาติ

มหาวิทยาลัยควรปรับแนวทางพัฒนาให้สอดคล้องกับนโยบายระดับชาติที่เกี่ยวข้อง ได้แก่:

- 1) ยุทธศาสตร์ชาติ 20 ปี ด้านการพัฒนาเทคโนโลยีดิจิทัล
- 2) แผนพัฒนาอุดมศึกษา ฉบับกระทรวง อว. ที่ผลักดันแนวคิด มหาวิทยาลัย 4.0
- 3) แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) โดยเฉพาะประเด็น Smart Campus และการใช้ Big Data
- 4) แผนปฏิบัติการรัฐบาลดิจิทัล (Digital Government Plan) ของ DGAที่เน้นการพัฒนาบริการอิเล็กทรอนิกส์ การเปิดเผยข้อมูล และความมั่นคงปลอดภัย

4.2 กรอบการทำงาน (Framework) ที่ควรใช้เป็นแนวอ้างอิง

กรอบการทำงานที่ควรใช้ในการออกแบบและวางระบบ Digital University มีดังนี้:

ตารางที่ 4 กรอบการทำงาน (Framework) ที่ควรใช้เป็นแนวอ้างอิง

กรอบการทำงาน	หน่วยงานต้นทาง	จุดเน้น
NIST CSF 2.0	National Institute of Standards and Technology (USA)	มาตรฐานการบริหารความมั่นคงปลอดภัยไซเบอร์ 6 ฟังก์ชัน (Govern–Recover)
DGA Digital Government Framework	สำนักงานรัฐบาลดิจิทัล (DGA)	บริการดิจิทัล, Open Data, Cloud, Data Governance
มหาวิทยาลัย 4.0 (อว.)	กระทรวง อว.	Flexible Learning, Data-driven Management, Engagement with Community
PDPA Compliance Framework	กระทรวงดิจิทัลฯ (ดีอีเอส)	การจัดการข้อมูลส่วนบุคคล, สิทธิของเจ้าของข้อมูล, การขอความยินยอม

มหาวิทยาลัยสามารถเลือกใช้กรอบเหล่านี้ร่วมกันในเชิงบูรณาการ โดยแบ่งความรับผิดชอบและบริหารจัดการเป็นระบบ ผ่านหน่วยงานกลาง เช่น คณะกรรมการขับเคลื่อนดิจิทัล หรือ War Room Digital Transformation

4.3 กฎหมายและระเบียบที่ต้องปฏิบัติตาม

เพื่อให้การดำเนินงานถูกต้องตามกฎหมาย และสามารถตรวจสอบได้ในภายหลัง มหาวิทยาลัยต้องดำเนินการภายใต้กฎหมายสำคัญเหล่านี้:



รูปที่ 1 แสดงแนวทางในการปฏิบัติงานตามกฎหมายของมหาวิทยาลัยดิจิทัล

- 1) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) → ต้องมี DPO, นโยบายคุ้มครองข้อมูล, และระบบสิทธิของเจ้าของข้อมูล
- 2) พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 → ต้องมี CSIRT, ระบบรายงานเหตุการณ์, การประเมินความเสี่ยง
- 3) พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 → รองรับการใช้อิเล็กทรอนิกส์, ลายมือชื่ออิเล็กทรอนิกส์
- 4) แนวทางจัดซื้อจัดจ้างด้าน IT จากกรมบัญชีกลาง → เพื่อให้สามารถดำเนินการโครงการได้โดยไม่ขัดต่อระเบียบพัสดุภาครัฐ

5. DIGITAL UNIVERSITY FRAMEWORK (DUF)

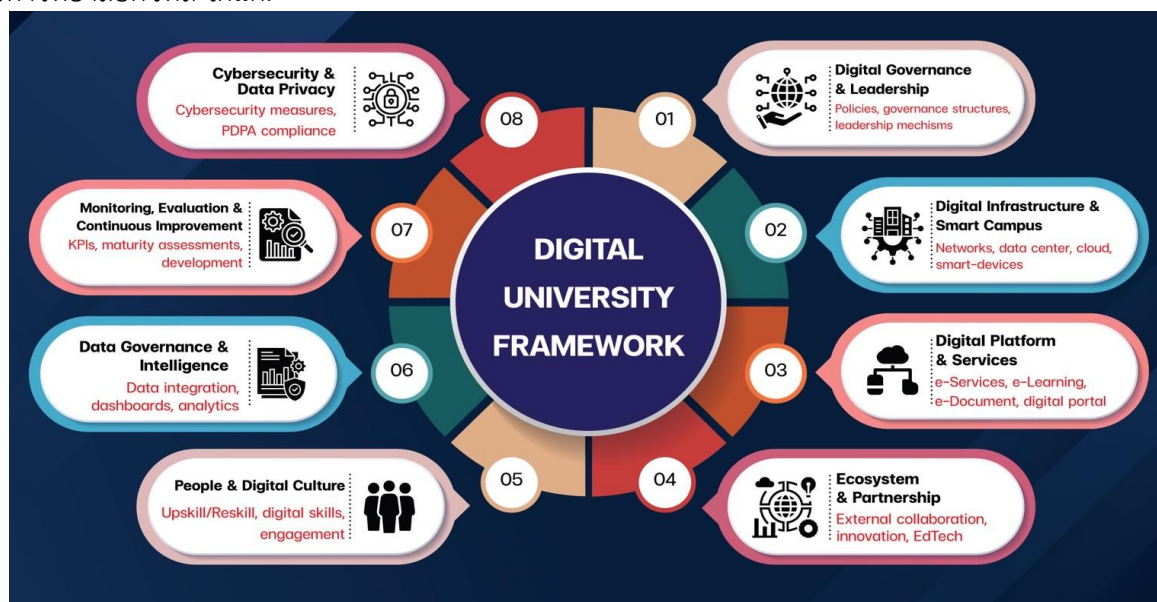
เมื่อแนวคิด Digital University กลายเป็นเป้าหมายเชิงยุทธศาสตร์ที่มหาวิทยาลัยทั่วประเทศต้องมุ่งสู่การดำเนินงานเพื่อให้ไปถึงเป้าหมายนั้นจำเป็นต้องมีกรอบแนวทาง ที่ชัดเจน ครอบคลุม และสามารถวัดผลได้ กรอบการทำงานนี้ไม่ได้เป็นเพียงแค่โครงสร้างแนวคิดทางทฤษฎี แต่เป็นระบบคิดเชิงกลยุทธ์ ที่ช่วยให้องค์กรสามารถ:

- 1) วางแผนการเปลี่ยนผ่านในแต่ละมิติ
- 2) จัดลำดับความสำคัญของโครงการ
- 3) แบ่งความรับผิดชอบให้แต่ละฝ่าย
- 4) ติดตามผลและประเมินความก้าวหน้าได้อย่างเป็นระบบ

ด้วยเหตุนี้ มหาวิทยาลัยวลัยลักษณ์ฯ จึงได้พัฒนา VRU Digital University Framework หรือ V-DUF ซึ่งเป็นกรอบการทำงานที่ปรับแต่งให้เหมาะสมกับบริบทของสถาบัน โดยอิงแนวคิดจากกรอบการทำงานระดับประเทศ เช่น DGA Digital Government Framework, มหาวิทยาลัย 4.0 (อว.) และ NIST CSF 2.0 สำหรับด้าน Cybersecurity

5.1 องค์ประกอบของ V-DUF

กรอบการทำงานV-DUF ประกอบด้วย 8 องค์ประกอบหลัก (8 Pillars) ซึ่งครอบคลุมการพัฒนาในทุกมิติของมหาวิทยาลัยดิจิทัล ได้แก่:



รูปที่ 2 แสดง VRU-DUF

ตารางที่ 5 แสดงแสดงองค์ประกอบทั้ง 8 ของ VRU-DUF

ลำดับ	องค์ประกอบหลัก	คำอธิบาย
1	Digital Governance & Leadership (DGL)	การกำกับดูแลและผู้นำเชิงดิจิทัล ต้องมีวิสัยทัศน์และนโยบายที่ชัดเจน
2	Digital Infrastructure & Smart Campus (DISC)	โครงสร้างพื้นฐานด้านเครือข่าย, ระบบ Cloud, IoT เพื่อรองรับระบบบริการดิจิทัล
3	Digital Platform & Services (DPS)	ระบบต่าง ๆ ที่ใช้งานทะเบียน, เรียนการสอน, บุคลากร และงานวิจัย
4	Ecosystem & Partnership (EP)	การสร้างความร่วมมือกับภาครัฐ เอกชน และชุมชน เพื่อร่วมขับเคลื่อนดิจิทัล
5	People & Digital Culture (PDC)	การสร้างทักษะ ทักษะคน และวัฒนธรรมองค์กรให้พร้อมเข้าสู่ยุคดิจิทัล
6	Data Governance & Intelligence (DGI)	การบริหารข้อมูลอย่างเป็นระบบ รวมถึงการวิเคราะห์และใช้ข้อมูลในการตัดสินใจ
7	Monitoring, Evaluation & Continuous Improvement (MEI)	การติดตามผล, ประเมินความก้าวหน้า และปรับปรุงอย่างต่อเนื่อง
8	Cybersecurity & Data Privacy (CDP)	ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล (PDPA, NIST CSF)

5.2 การเชื่อมโยงกับมาตรฐาน / แนวนโยบายที่เกี่ยวข้อง

ในการพัฒนามหาวิทยาลัยดิจิทัลให้มีทิศทางที่ชัดเจน เป็นระบบ และสามารถตรวจสอบได้ จำเป็นอย่างยิ่งที่แผนงานจะต้องเชื่อมโยงกับ มาตรฐานกลางและนโยบายระดับชาติ ที่ได้รับการยอมรับ ทั้งในเชิงกฎหมาย มาตรฐานเทคโนโลยี และแนวปฏิบัติจากหน่วยงานกำกับดูแล เพื่อให้มั่นใจว่าการดำเนินงานมีความ

ถูกต้อง ครอบคลุม และสามารถขับเคลื่อนไปพร้อมกับหน่วยงานภาครัฐอื่น ๆ ได้อย่างกลมกลืน ดังแสดงในตารางที่ 6

ตารางที่ 6 แสดงการเชื่อมโยงกับมาตรฐาน / แนวนโยบายที่เกี่ยวข้อง

องค์ประกอบ	กระทรวง อว. (มหาวิทยาลัย 4.0)	DGA (Digital Gov)	DE / สดช. (DES Strategy)	หมายเหตุ
1. Digital Governance & Leadership	☒ วิสัยทัศน์/ นโยบายดิจิทัล	☒ Digital Governance Model	◇ ไม่เน้น	โครงสร้าง คณะกรรมการดิจิทัล ต้องมี
2. Digital Infrastructure & Smart Campus	☒ Smart Campus / IoT	☒ Cloud First Policy	☒ Network, 5G, Cloud Edge	ต้องอิง Cloud+On- Prem ตาม แนวนโยบาย
3. Digital Platform & Services	☒ e-Learning, e- Office	☒ e-Services, SSO	☒ Digital Government APIs	สอดคล้องกับ บริการ ดิจิทัลภาครัฐ
4. People & Digital Culture	☒ Digital Competency อาจารย์/นักศึกษา	◇ ไม่เน้น	☒ Digital Literacy, Reskill/UpSkill	ควรมีแผนฝึกอบรมและ วัดผล
5. Data Governance & Intelligence	☒ Learning Analytics, Dashboard	☒ Data Governance Manual	☒ Big Data / AI Strategy	ควรรอง DGA Data Standards
6. Cybersecurity & Data Privacy	◇ (บางส่วน)	☒ PDPA Compliance, CSF	☒ พ.ร.บ. Cybersecurity 2562	สำคัญมาก ต้องมี CSIRT, Risk Plan
7. Ecosystem & Partnership	☒ University- Industry Linkage	◇ ไม่เน้น	☒ Public-Private Innovation Ecosystem	เสริมด้วย MOU กับ Startup/EdTech
8. Monitoring & Continuous Improvement	☒ QA, EdPEX, Maturity Model	☒ Digital Gov Maturity	☒ ตัวชี้วัดตามแผน ระดับชาติ	ต้องกำหนด KPI ราย ด้านในแต่ละปี

5.3 สรุปความสอดคล้องของ V-DUF กับแผนของประเทศ

เพื่อให้การดำเนินงานตามกรอบ V-DUF เป็นไปอย่างมีทิศทาง และสามารถรองรับการตรวจสอบในระดับนโยบายได้อย่างรอบด้าน จึงจำเป็นต้องแสดงให้เห็นถึงความสอดคล้องระหว่างองค์ประกอบของ V-DUF กับ แผนระดับประเทศและกรอบยุทธศาสตร์สำคัญ ไม่ว่าจะเป็นยุทธศาสตร์ชาติ 20 ปี, แผนปฏิรูปมหาวิทยาลัย 4.0, แผนดิจิทัลภาครัฐ (DGA) หรือกรอบมาตรฐานความมั่นคงปลอดภัยไซเบอร์ NIST CSF 2.0

การเชื่อมโยงเหล่านี้ไม่เพียงสะท้อนว่าแผนของมหาวิทยาลัยเดินตามแนวนโยบายของรัฐ แต่ยังเป็นหลักประกันว่าแผนจะสามารถขอรับการสนับสนุนงบประมาณ ตอบโจทย์การประเมิน และพัฒนาได้ในระดับที่เทียบเคียงกับมาตรฐานของประเทศ

ตารางที่ 7 แสดงสรุปความสอดคล้องของ V-DUF กับแผนของประเทศ

ประเด็น	ผลลัพธ์
สอดคล้องกับแผนพัฒนาอุดมศึกษาของ อว.	☒ ครบทั้ง 8 ด้าน

สอดคล้องกับ Digital Government Plan ของ DGA	☒ ครอบคลุม 7/8 ด้าน (People & Digital Culture ไม่นับ)
สอดคล้องกับ Digital Economy Strategy ของ สดช.	☒ ครบทั้ง 8 ด้าน

5.4 การนำ V-DUF ไปใช้ในระดับปฏิบัติ

กรอบการทำงานนี้จะถูกใช้เป็น กรอบอ้างอิงหลัก ในการจัดทำ:

- 1) แผนแม่บทการพัฒนาดิจิทัลระดับมหาวิทยาลัย
- 2) แผนการดำเนินการรายปี/รายเดือนของแต่ละหน่วยงาน
- 3) การจัดทำโครงการดิจิทัล เช่น ระบบ SSO, e-Document, Data Lake
- 4) การติดตามผลด้วยเครื่องมือดิจิทัล เช่น Dashboard หรือ Maturity Model

โดยในแต่ละองค์ประกอบ จะมีการกำหนดเป้าหมายเชิงกลยุทธ์ กิจกรรมหลัก และตัวชี้วัด (KPI) อย่างเป็นรูปธรรม ซึ่งจะกล่าวถึงในหัวข้อต่อไป

5.5 องค์ประกอบของ VRU-DUF

เพื่อให้การขับเคลื่อนมหาวิทยาลัยวไลยอลงกรณ์ฯ ไปสู่ความเป็นมหาวิทยาลัยดิจิทัล (Digital University) เป็นไปอย่างเป็นระบบ ครอบคลุม และสามารถติดตามผลได้อย่างมีประสิทธิภาพ จึงได้กำหนดกรอบแนวทางการดำเนินงานที่เรียกว่า VRU Digital University Framework (VRU-DUF) ซึ่งประกอบด้วย 8 องค์ประกอบหลัก ที่สะท้อนทั้งมิติด้านเทคโนโลยี องค์กร บุคลากร และความร่วมมือ

ในหัวข้อนี้ จะนำเสนอรายละเอียดของแต่ละองค์ประกอบอย่างเป็นระบบ พร้อมแนวทางการดำเนินการที่สามารถประยุกต์ใช้ได้จริงในบริบทของมหาวิทยาลัย

5.5.1 องค์ประกอบที่ 1: Digital Governance & Leadership (DGL)

การเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัลจำเป็นต้องมีการกำกับดูแลที่ดี (Governance) และผู้นำที่มีวิสัยทัศน์ด้านดิจิทัล (Digital Leadership) เพราะเทคโนโลยีไม่สามารถสร้างผลลัพธ์ได้ หากขาดแนวนโยบายที่ชัดเจน โครงสร้างการบริหารที่เปิดกว้าง และบุคลากรที่กล้าตัดสินใจเชิงกลยุทธ์

Digital Governance & Leadership จึงถือเป็น หัวใจ ของกรอบการทำงานVRU-DUF ซึ่งจะทำหน้าที่กำหนดทิศทาง ดึงพลังจากทุกภาคส่วน และผลักดันการพัฒนาให้เกิดขึ้นจริง

▪ เป้าหมายหลัก

- มีผู้นำเชิงนโยบายและปฏิบัติการที่สามารถขับเคลื่อนมหาวิทยาลัยเข้าสู่ยุคดิจิทัล
- มีกลไกบริหารจัดการและกำกับติดตามโครงการดิจิทัลอย่างเป็นระบบ
- มียุทธศาสตร์ดิจิทัลและกรอบนโยบายที่สอดคล้องกับแผนชาติ

▪ แนวทางการดำเนินงาน

- 1) แต่งตั้งคณะกรรมการขับเคลื่อนดิจิทัล (Digital Transformation Committee) ประกอบด้วยผู้บริหารระดับสูง และตัวแทนจากทุกหน่วยงานที่เกี่ยวข้อง โดยมีอำนาจหน้าที่ชัดเจนในการกำหนดนโยบาย กำกับโครงการ และรายงานผลต่อผู้บริหารสูงสุด
- 2) แต่งตั้งผู้บริหารด้านดิจิทัล (CDO หรือ CIO) เพื่อดูแลยุทธศาสตร์ดิจิทัลทั้งองค์กร ทำหน้าที่เป็นจุดประสานระหว่างภาคนโยบายกับภาคปฏิบัติ
- 3) จัดทำแผนแม่บทดิจิทัล (Digital Master Plan)

ครอบคลุมเป้าหมาย แผนงาน งบประมาณ และดัชนีชี้วัด เพื่อใช้เป็นพิมพ์เขียวระยะ 3-5 ปี

- 4) จัดตั้งศูนย์ปฏิบัติการกลาง (Digital War Room) เพื่อทำหน้าที่ติดตาม วิเคราะห์ และสนับสนุนการขับเคลื่อนทุกมิติผ่าน Dashboard กลาง
- 5) กำหนดดัชนีชี้วัด (Digital KPI) เช่น ระยะเวลาอนุมัติเอกสารผ่านระบบ, อัตราการใช้บริการออนไลน์, ระดับความพึงพอใจผู้ใช้งาน

ตารางที่ 7 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Digital Governance, Executive Leadership
มหาวิทยาลัย 4.0 (อว.)	University Management, Policy Integration
NIST CSF 2.0	Govern Function (ใหม่ในเวอร์ชัน 2.0)

ตารางที่ 8 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 1

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	สัดส่วนหน่วยงานที่จัดทำแผนดิจิทัลรายปี (Digital Action Plan)	80	%	สะท้อนระดับความครอบคลุมการวางแผนรายหน่วย
2	จำนวนครั้งการประชุมคณะกรรมการขับเคลื่อน V-DUF ต่อปี	4	ครั้ง	วัดความสม่ำเสมอของการติดตามระดับยุทธศาสตร์
3	ระยะเวลาการอนุมัติ/ดำเนินโครงการดิจิทัล (เฉลี่ย)	30	วัน	วัดความคล่องตัวในการตัดสินใจและบริหารจัดการ
4	จำนวนหน่วยงานที่แต่งตั้ง Digital Ambassador หรือผู้ประสานงานดิจิทัล	70	หน่วยงาน	สะท้อนโครงสร้างความพร้อมระดับปฏิบัติการ
5	สัดส่วนโครงการดิจิทัลที่มีการรายงานผลต่อผู้บริหารภายในระยะเวลาที่กำหนด	90	%	วัดความเข้มแข็งของระบบติดตามผลโครงการ

องค์ประกอบนี้มุ่งวัดความเข้มแข็งของ ระบบบริหารจัดการเชิงดิจิทัล ของมหาวิทยาลัย ตั้งแต่ระดับนโยบาย ยุทธศาสตร์ ไปจนถึงกลไกสนับสนุนระดับปฏิบัติการ เพื่อให้การขับเคลื่อน Digital Transformation ไม่เป็นเพียงคำประกาศ แต่มีการวางแผนและลงมือทำอย่างเป็นระบบ ตัวชี้วัดแต่ละตัวมีรายละเอียดดังนี้:

KPI 1: สัดส่วนหน่วยงานที่จัดทำแผนดิจิทัลรายปี (Digital Action Plan) วัดจากจำนวนหน่วยงานที่มีการจัดทำแผนรายปีเกี่ยวกับการนำเทคโนโลยีดิจิทัลมาใช้พัฒนาการทำงาน เทียบกับจำนวนหน่วยงานทั้งหมด เช่น คณะ, สำนัก, ศูนย์ ต่าง ๆ มีแผนเชิงปฏิบัติการรองรับแผนแม่บท

KPI 2: จำนวนครั้งการประชุมคณะกรรมการขับเคลื่อน V-DUF ต่อปี วัดความต่อเนื่องของการติดตาม และตัดสินใจในระดับยุทธศาสตร์ โดยคณะกรรมการนี้มีหน้าที่ติดตามประเมินผลการดำเนินงาน และปรับแนวทางให้สอดคล้องกับสถานการณ์

KPI 3: ระยะเวลาการอนุมัติ/ดำเนินโครงการดิจิทัล (เฉลี่ย) วัดความเร็วในการตอบสนองต่อโครงการด้านดิจิทัล เช่น ระยะเวลาจากการเสนอ TOR หรือแผนงานจนถึงอนุมัติและเริ่มดำเนินการ ซึ่งสะท้อนถึงความคล่องตัวของระบบบริหารจัดการ

KPI 4: จำนวนหน่วยงานที่แต่งตั้ง Digital Ambassador หรือผู้ประสานงานดิจิทัล วัดการกระจายบทบาทความรับผิดชอบลงสู่ระดับหน่วยงาน โดยการแต่งตั้งเจ้าหน้าที่ที่มีหน้าที่ส่งเสริมการใช้เทคโนโลยี และเป็นตัวกลางระหว่างหน่วยงานกับศูนย์ดิจิทัลกลาง

KPI 5: สัดส่วนโครงการดิจิทัลที่มีการรายงานผลต่อผู้บริหารภายในระยะเวลาที่กำหนด วัดคุณภาพของระบบติดตามและรายงานผล เช่น โครงการที่ได้รับงบประมาณ ต้องมีรายงานผล/ความคืบหน้าเข้าสู่ระบบกลางหรือที่ประชุมภายในกรอบเวลาที่กำหนด (เช่น รายไตรมาส)

5.5.2 องค์ประกอบที่ 2: Digital Infrastructure & Smart Campus (DISC)

การพัฒนาาระบบโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ เป็นรากฐานสำคัญของการขับเคลื่อนมหาวิทยาลัยดิจิทัลอย่างยั่งยืน หากไม่มีระบบเครือข่ายที่เสถียร อุปกรณ์ที่ทันสมัย หรือศูนย์ข้อมูลที่ปลอดภัย ก็ย่อมเป็นการยากที่จะให้บริการแบบออนไลน์ หรือสร้างสภาพแวดล้อมการเรียนรู้และทำงานที่ยืดหยุ่น ทันสมัยได้อย่างแท้จริง

Digital Infrastructure & Smart Campus จึงเป็นองค์ประกอบที่เน้นการจัดเตรียม พื้นที่ดิจิทัล ให้พร้อมสำหรับรองรับระบบบริการดิจิทัลทั้งหมด ไม่ว่าจะเป็นระบบบริหารจัดการ การเรียนการสอน หรือการใช้ข้อมูลขนาดใหญ่และปัญญาประดิษฐ์ในอนาคต

- เป้าหมายหลัก
 - 1) มีโครงข่ายอินเทอร์เน็ตและ Wi-Fi ครอบคลุมทุกพื้นที่ใช้งานในมหาวิทยาลัย
 - 2) มี Data Center และ Cloud Infrastructure ที่สามารถรองรับระบบงานต่าง ๆ อย่างปลอดภัย
 - 3) มีอุปกรณ์ดิจิทัลและ IoT ที่ช่วยสร้างสิ่งแวดล้อมแบบ Smart Campus
 - 4) ระบบโครงสร้างพื้นฐานสอดคล้องกับมาตรฐานความมั่นคงปลอดภัย
- แนวทางการดำเนินงาน
 - 1) อัปเดตระบบเครือข่าย (Network Modernization) ปรับปรุงระบบสายสัญญาณและจุดกระจายสัญญาณ Wi-Fi ให้ครอบคลุมทั่วทั้งมหาวิทยาลัย รวมถึงหอพัก และพื้นที่บริการชุมชน
 - 2) จัดตั้งศูนย์ข้อมูล (Data Center) และเชื่อมโยงระบบคลาวด์ (Hybrid Cloud) ใช้โซลูชันแบบ Cloud First โดยผสาน Cloud ภาครัฐ (G-Cloud) กับ Local Server เพื่อให้ระบบมีความยืดหยุ่นและปลอดภัย
 - 3) ติดตั้งอุปกรณ์ IoT และระบบ Smart Facility เช่น ระบบตรวจจับพลังงาน, กล้องวงจรปิดอัจฉริยะ, ระบบเปิด-ปิดไฟอัตโนมัติ หรือระบบนับจำนวนนักศึกษาบริเวณอาคารเรียน
 - 4) เตรียมระบบสำรองข้อมูล (Backup & Disaster Recovery) เพื่อรองรับเหตุการณ์ฉุกเฉิน และป้องกันการสูญหายของข้อมูลสำคัญ
 - 5) จัดหาครุภัณฑ์ดิจิทัลที่จำเป็น เช่น คอมพิวเตอร์แม่ข่าย (Server), Firewall, Storage NAS, เครื่องมือพัฒนา AI, อุปกรณ์ฝึกสอนดิจิทัล

ตารางที่ 9 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Digital Infrastructure, Government Cloud
มหาวิทยาลัย 4.0 (อว.)	Smart Campus, Digital Resource
NIST CSF 2.0	Protect Function (ระบบพื้นฐานปลอดภัย)

ตารางที่ 10 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 2

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	ความครอบคลุมของ Wi-Fi ในพื้นที่ใช้งานหลัก	90%	ร้อยละของพื้นที่	พื้นที่รวมอาคารเรียน ห้องสมุด หอพัก และสำนักงาน
2	จำนวนอุปกรณ์ IoT/Smart Facility ที่ติดตั้งใช้งานจริง	≥ 10 รายการ	รายการ	เช่น กล้องอัจฉริยะ, ระบบควบคุมแสง, ระบบตรวจจับคน

3	ความพร้อมของระบบสำรองข้อมูล (Backup System)	ต้องมี	มี/ไม่มี	ครอบคลุมระบบสารสนเทศหลัก เช่น ทะเบียน, การเงิน
4	ความพร้อมของระบบ Disaster Recovery (DR Site)	อย่างน้อย Tier 2	ระดับความพร้อม	อิงมาตรฐาน Data Center Readiness
5	จำนวนระบบหลักที่เชื่อมต่อกับ Cloud Infrastructure	≥ 3 ระบบ	ระบบ	เช่น e-Document, LMS, SSO
6	จำนวนระบบที่ย้ายไป G-Cloud หรือ Cloud Server	≥ 5 ระบบ	ระบบ	สอดคล้องกับ Cloud First Policy ของภาครัฐ

องค์ประกอบนี้เป็นรากฐานของการขับเคลื่อนมหาวิทยาลัยดิจิทัล เพราะไม่ว่าจะพัฒนาระบบงาน การเรียนการสอน หรือบริการใด ๆ ล้วนต้องอาศัยโครงสร้างพื้นฐานด้านดิจิทัลที่มั่นคง ครอบคลุม และพร้อมใช้งาน ตัวชี้วัดเหล่านี้จะสะท้อนความพร้อมของมหาวิทยาลัยในระดับโครงสร้างพื้นฐาน ดังนี้:

KPI 1: ความครอบคลุมของ Wi-Fi ในพื้นที่ใช้งานหลัก วัดจากเปอร์เซ็นต์ของพื้นที่ที่มีสัญญาณ Wi-Fi ครอบคลุม เช่น อาคารเรียน ห้องสมุด หอพัก และสำนักงาน เพื่อให้บุคลากรและนักศึกษาเข้าถึงระบบต่าง ๆ ได้ทุกที่ทุกเวลา

KPI 2: จำนวนอุปกรณ์ IoT/Smart Facility ที่ติดตั้งใช้งานจริง วัดจากการใช้อุปกรณ์อัจฉริยะ เช่น กล้องวงจรปิดอัจฉริยะ, ระบบควบคุมไฟฟ้า, ระบบตรวจจับคน เพื่อยกระดับความปลอดภัยและประสิทธิภาพของอาคารสถานที่

KPI 3: ความพร้อมของระบบสำรองข้อมูล (Backup System) วัดจากการมีระบบสำรองข้อมูลที่ครอบคลุมระบบสำคัญ เช่น ฐานข้อมูลนักศึกษา, ระบบเงินเดือน เพื่อรองรับเหตุการณ์ฉุกเฉิน เช่น ไฟฟ้าดับ หรือระบบล่ม

KPI 4: ความพร้อมของระบบ Disaster Recovery (DR Site) วัดระดับความพร้อมของศูนย์สำรองระบบ (เช่น Tier 2 ตามมาตรฐาน Data Center) ที่สามารถเปิดใช้ระบบต่อเนื่องในกรณีเกิดภัยพิบัติ

KPI 5: จำนวนระบบหลักที่เชื่อมต่อกับ Cloud Infrastructure วัดจำนวนระบบสารสนเทศที่ย้ายจากการติดตั้งแบบเดิม (On-premise) ไปยัง Cloud เช่น ระบบจัดการเอกสาร, LMS, ระบบบัญชี/SSO ซึ่งเพิ่มความยืดหยุ่นและรองรับการใช้งานระยะไกล

KPI 6: จำนวนระบบที่ย้ายไป G-Cloud หรือ Cloud Server วัดจากจำนวนระบบที่ปรับเปลี่ยนโครงสร้างให้สอดคล้องกับ Cloud First Policy ของรัฐบาล เช่น การย้ายระบบบางส่วนไปยัง G-Cloud ของภาครัฐหรือบริการ Cloud Infrastructure อื่นที่มีมาตรฐาน

5.5.3 องค์ประกอบที่ 3: Digital Platform & Services (DPS)

หลังจากที่มหาวิทยาลัยสามารถวางรากฐานทางด้านโครงสร้างพื้นฐานดิจิทัล (Digital Infrastructure) ได้อย่างมั่นคงแล้ว ขั้นตอนต่อไปที่จะทำให้เกิดการเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัลเกิดขึ้นจริงในสายตาของผู้ใช้งาน ได้แก่ การออกแบบและให้บริการผ่าน แพลตฟอร์มดิจิทัล (Digital Platform) ที่ตอบโจทย์การใช้งานของทุกกลุ่มเป้าหมาย ทั้งนักศึกษา อาจารย์ บุคลากร และผู้บริหาร

องค์ประกอบ Digital Platform & Services (DPS) จึงเป็นเสมือน “หน้าตา” ของมหาวิทยาลัยดิจิทัล โดยรวมศูนย์การให้บริการสารสนเทศในด้านต่าง ๆ ไม่ว่าจะเป็นระบบทะเบียน, การเรียนการสอน, บุคลากร, การเงิน, วิจัย, และการให้บริการนักศึกษา – ทั้งหมดต้องสามารถใช้งานได้อย่างสะดวก ปลอดภัย และเชื่อมโยงถึงกันได้

แพลตฟอร์มเหล่านี้ควรถูกพัฒนาให้รองรับ การเชื่อมต่อด้วย API กลาง มีการออกแบบตามกรอบ Enterprise Architecture (EA) และรองรับ มาตรฐานการแลกเปลี่ยนข้อมูลแบบเปิด (Open Standard) เช่น JSON, XML, OAuth, SAML เพื่อเพิ่มความสามารถในการบูรณาการระบบต่าง ๆ เข้าด้วยกัน ทั้งภายในและภายนอกมหาวิทยาลัย

นอกจากนี้ ผู้ใช้งานควรสามารถเข้าถึงบริการต่าง ๆ ได้จาก Web Portal หรือ SSO เพียงหนึ่งเดียว พร้อมทั้งมีแอปพลิเคชันที่ใช้งานได้ทั้งบนมือถือและเว็บ เพื่อเพิ่มความสะดวกในการเข้าถึง ไม่ว่าจะอยู่ที่ไหน เวลาใดก็ตาม ทั้งหมดนี้จะช่วยลดความซับซ้อนของระบบ เพิ่มประสิทธิภาพการให้บริการ และยกระดับประสบการณ์ผู้ใช้อย่างแท้จริง

■ เป้าหมายหลัก

- 1) ให้บริการภารกิจหลักของมหาวิทยาลัยผ่านระบบดิจิทัลอย่างทั่วถึง ครอบคลุม และเข้าถึงได้ง่าย ทั้งในด้านการเรียนการสอน การวิจัย การบริหารจัดการ และบริการนักศึกษา
- 2) เชื่อมโยงข้อมูลและระบบต่าง ๆ ผ่าน API และมาตรฐานกลาง (Open Standard) เพื่อให้เกิดการให้บริการแบบไร้รอยต่อ (Seamless Services) และลดความซ้ำซ้อนในการพัฒนาระบบ
- 3) ลดการใช้เอกสารแบบเดิม (Paperless) โดยเปลี่ยนเป็นกระบวนการดิจิทัลเต็มรูปแบบ เช่น การยื่นคำร้อง, การแจ้งซ่อม, การขอเอกสาร ผ่านระบบออนไลน์
- 4) จัดทำ Web Portal และระบบ SSO (Single Sign-On) เพื่อให้ผู้ใช้สามารถเข้าถึงทุกระบบที่จำเป็นได้จากจุดเดียว ด้วยความสะดวก รวดเร็ว และปลอดภัย
- 5) ส่งเสริมประสบการณ์ผู้ใช้ที่ดี ด้วยการออกแบบแพลตฟอร์มที่ใช้งานง่าย รองรับอุปกรณ์พกพา และสอดคล้องกับพฤติกรรมของผู้เรียนและบุคลากรในยุคดิจิทัล
- 6) รองรับการเรียนรู้และการบริหารจัดการที่ยืดหยุ่น ด้วยแพลตฟอร์มที่สามารถปรับขยาย (scalable) และรองรับการเชื่อมโยงภายนอก เช่น G-Cloud หรือระบบสนับสนุนอื่นของภาครัฐ

■ แนวทางการดำเนินงาน

- 1) พัฒนาระบบบริการดิจิทัลให้ครอบคลุมทุกภารกิจหลักของมหาวิทยาลัย เช่น ระบบทะเบียน (Reg), ระบบสารบรรณอิเล็กทรอนิกส์ (e-Document), ระบบบุคลากร (HR), การเงิน (Finance), ระบบเรียนการสอน (LMS), ระบบงานวิจัย และระบบบริการนักศึกษา ให้รองรับการใช้งานในทุกกลุ่มผู้ใช้
- 2) ออกแบบระบบให้เชื่อมโยงกันได้ผ่าน API และรองรับมาตรฐานเปิด (Open Standard) ใช้รูปแบบ เช่น JSON, XML, OAuth, SAML เพื่อเชื่อมโยงข้อมูลระหว่างระบบภายใน และสามารถต่อยอดสู่ระบบภายนอก เช่น G-Cloud, ระบบของหน่วยงานภาครัฐอื่น ๆ
- 3) จัดทำ Enterprise Architecture (EA) เพื่อแสดงโครงสร้างและความสัมพันธ์ระหว่างระบบสารสนเทศทั้งหมด ช่วยให้การพัฒนาและเชื่อมต่อระบบเกิดขึ้นอย่างมีทิศทาง ไม่ซ้ำซ้อน
- 4) พัฒนา Web Portal และระบบ Single Sign-On (SSO) ให้ผู้ใช้งานสามารถเข้าถึงระบบบริการต่าง ๆ ได้จากทางเข้าเดียว ไม่ต้องจดจำหลายรหัสผ่าน และสามารถใช้งานได้จากทั้งคอมพิวเตอร์และอุปกรณ์พกพา
- 5) พัฒนา Mobile/Web Application สำหรับบริการที่ใช้งานบ่อย เช่น ระบบแจ้งซ่อม, การขอเอกสาร, การจองห้องเรียน, การยื่นคำร้อง ฯลฯ เพื่อเพิ่มความสะดวกในการเข้าถึงและลดการใช้กระดาษ (Paperless)
- 6) ติดตามและประเมินการใช้งานระบบอย่างต่อเนื่อง ผ่านตัวชี้วัดการใช้งานจริง เช่น ปริมาณผู้ใช้ ความพึงพอใจ และประสิทธิภาพของระบบ เพื่อใช้ข้อมูลในการปรับปรุงประสบการณ์ผู้ใช้

- 7) เชื่อมโยงระบบที่จำเป็นกับโครงสร้าง Cloud หรือ G-Cloud เพื่อลดภาระในการดูแลระบบภายใน และเพิ่มความยืดหยุ่นในการขยายบริการ รวมถึงตอบสนองนโยบาย Cloud First ของภาครัฐ

ตารางที่ 11 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	e-Service, SSO, Open API
มหาวิทยาลัย 4.0 (อว.)	Flexible Learning Platform, Digital Service
NIST CSF 2.0	Identify / Protect (ระบบบริการและผู้ใช้ที่ปลอดภัย)

ตารางที่ 12 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 3

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	จำนวนระบบสารสนเทศหลักที่ให้บริการผ่านแพลตฟอร์มดิจิทัล	≥ 6 ระบบ	ระบบ	เช่น Reg, HR, e-Doc, LMS, Finance, Research
2	จำนวนระบบที่เชื่อมโยงผ่าน API กลาง	≥ 10 ระบบ	ระบบ	ระบบที่มีการเชื่อมต่อผ่าน API Gateway
3	การจัดทำ Enterprise Architecture (EA) ที่แสดงความสัมพันธ์ของระบบ	ต้องมี	มี/ไม่มี	ใช้เป็นแผนภาพแสดงการเชื่อมโยงระบบทั้งหมด
4	สัดส่วนระบบสารสนเทศที่รองรับมาตรฐานการแลกเปลี่ยนข้อมูล (Open Standard)	≥ 80%	ร้อยละของระบบ	เช่น JSON, XML, OAuth, SAML
5	จำนวนบริการที่ผู้ใช้เข้าถึงผ่าน Web Portal หรือ SSO เดียว	≥ 10 บริการ	บริการ	เช่น ตรวจสอบผลการเรียน, ขอนหนังสือรับรอง, ยื่นคำร้อง
6	ระดับความพึงพอใจของผู้ใช้ต่อระบบแพลตฟอร์มดิจิทัล	≥ 4.0	คะแนนเฉลี่ย	วัดจากแบบประเมินความพึงพอใจรายไตรมาส

องค์ประกอบนี้มุ่งเน้นการพัฒนาแพลตฟอร์มดิจิทัลที่มีประสิทธิภาพ ใช้งานง่าย เชื่อมโยงถึงกันได้ และตอบโจทย์ทุกกลุ่มเป้าหมายในมหาวิทยาลัย โดยตัวชี้วัดที่กำหนดขึ้นสะท้อนถึงทั้งมิติด้าน “ปริมาณการให้บริการ”, “คุณภาพของโครงสร้างระบบ”, และ “ประสบการณ์ผู้ใช้” ดังนี้:

KPI 1: จำนวนระบบสารสนเทศหลักที่ให้บริการผ่านแพลตฟอร์มดิจิทัล วัดจำนวนระบบหลักที่พัฒนาขึ้นและเปิดให้ใช้งานผ่าน Web หรือ Mobile Application โดยครอบคลุมภารกิจหลัก เช่น ระบบทะเบียน (Reg), ระบบบุคลากร (HR), ระบบ e-Document, ระบบการเรียนการสอน (LMS) และระบบการเงิน

KPI 2: จำนวนระบบที่เชื่อมโยงผ่าน API กลาง วัดความสามารถของระบบในการเชื่อมต่อผ่าน API Gateway โดยเน้นเฉพาะระบบที่มีการเชื่อมต่อข้อมูลกันจริง เพื่อให้เกิดการให้บริการแบบไร้รอยต่อ เช่น การดึงข้อมูลนักศึกษาไปยังหลายระบบโดยไม่ต้องกรอกซ้ำ

KPI 3: การจัดทำ Enterprise Architecture (EA) เป็นการจัดทำแผนภาพแสดงความสัมพันธ์ระหว่างระบบสารสนเทศ เพื่อให้เห็นภาพรวมของการบูรณาการ ช่วยให้การพัฒนาระบบใหม่ไม่เกิดความซ้ำซ้อน

KPI 4: สัดส่วนระบบสารสนเทศที่รองรับมาตรฐานการแลกเปลี่ยนข้อมูล (Open Standard) วัดจากจำนวนระบบที่ใช้มาตรฐานกลางในการแลกเปลี่ยนข้อมูล เช่น JSON, XML, OAuth, SAML ซึ่งทำให้ระบบต่าง ๆ เชื่อมต่อกันได้ง่าย และมีความปลอดภัย

KPI 5: จำนวนบริการที่ผู้ใช้เข้าถึงผ่าน Web Portal หรือ SSO เดียว วัดจากจำนวนบริการที่รวมไว้ในจุดเข้าระบบกลาง (Portal) โดยผู้ใช้ไม่ต้องล็อกอินหลายครั้ง เช่น การตรวจสอบผลการเรียน การขอเอกสารการยื่นคำร้องต่าง ๆ

KPI 6: ระดับความพึงพอใจของผู้ใช้ต่อระบบแพลตฟอร์มดิจิทัล วัดจากแบบสอบถามหรือแบบประเมินออนไลน์ เพื่อสะท้อนประสบการณ์ผู้ใช้จริง เช่น ความง่ายในการใช้งาน ความรวดเร็ว และความเสถียรของระบบ

5.5.4 องค์ประกอบที่ 4: Ecosystem & Partnership (EP)

การพัฒนามหาวิทยาลัยดิจิทัลไม่สามารถเกิดขึ้นได้ด้วยการดำเนินงานภายในเพียงลำพัง การสร้างเครือข่ายความร่วมมือและระบบนิเวศดิจิทัล (Digital Ecosystem) ที่เชื่อมโยงกับภาครัฐ เอกชน ชุมชน และภาคการศึกษาร่วมกัน จึงกลายเป็นหัวใจสำคัญในการผลักดันให้เกิดนวัตกรรมดิจิทัลที่แท้จริง และตอบโจทย์ความต้องการของสังคมในทุกระดับ

องค์ประกอบ Ecosystem & Partnership (EP) สะท้อนบทบาทของมหาวิทยาลัยในฐานะ "แพลตฟอร์มของการพัฒนา" ซึ่งต้องมีพันธมิตรทางเทคโนโลยี ผู้สนับสนุนทุนวิจัย ภาควิชาการ ผู้ใช้เทคโนโลยีจริงในพื้นที่ และผู้มีส่วนได้ส่วนเสียหลากหลายกลุ่ม ที่ร่วมกันขับเคลื่อนความเปลี่ยนแปลงผ่านระบบดิจิทัล โดยเฉพาะในบริบทของมหาวิทยาลัยท้องถิ่นที่มีพันธกิจเพื่อชุมชน การดำเนินงานด้านความร่วมมือจึงควรเน้นไปที่โครงการที่ก่อให้เกิดผลลัพธ์เชิงสังคมอย่างเป็นรูปธรรม

ตัวอย่างของความร่วมมือที่ตอบโจทย์แนวคิดนี้ เช่น โครงการ Smart Farming ร่วมกับเกษตรกรในพื้นที่, ระบบ OTOP Online ที่ช่วยผู้ประกอบการท้องถิ่นเข้าถึงตลาดดิจิทัล, หรือการพัฒนา แพลตฟอร์มเมืองอัจฉริยะ (Smart City) ระดับตำบล ที่ออกแบบร่วมกับภาคีทั้งภาครัฐและเอกชน สิ่งเหล่านี้ไม่เพียงแต่เป็นการนำเทคโนโลยีเข้าไปใช้ในพื้นที่จริงเท่านั้น แต่ยังเป็นเวทีให้นักศึกษาและบุคลากรได้ลงมือสร้างนวัตกรรมที่มีผลกระทบต่อชุมชนอย่างแท้จริง

■ เป้าหมายหลัก

- 1) สร้างความร่วมมือกับหน่วยงานภายนอกที่มีศักยภาพด้านเทคโนโลยี นวัตกรรม หรือการจัดการดิจิทัล เพื่อเสริมจุดแข็งของมหาวิทยาลัย
- 2) พัฒนาระบบนิเวศ (Ecosystem) ภายในมหาวิทยาลัย โดยใช้ความร่วมมือเหล่านี้เป็นกลไกเร่งการเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัล
- 3) สนับสนุนให้เกิดแพลตฟอร์มหรือบริการดิจิทัลใหม่ ๆ ผ่านการพัฒนา/ถ่ายทอดเทคโนโลยีจากภาคี
- 4) สร้างเวทีความร่วมมือที่เปิดให้เกิดการ Co-Create ระหว่างบุคลากร นักศึกษา และภาคเอกชน
- 5) ติดตามและวัดผลลัพธ์ของความร่วมมือว่าเชื่อมโยงกับเป้าหมายด้าน Digital University ได้อย่างเป็นรูปธรรม

■ แนวทางการดำเนินงาน

- 1) สร้างแผนที่พันธมิตรเชิงกลยุทธ์ (Strategic Partnership Map) ระบุประเภทองค์กรภายนอกที่จำเป็นต่อการเสริมความสามารถด้านดิจิทัล เช่น บริษัทด้าน Cloud, Security, Big Data, AI, EdTech และจัดลำดับความสำคัญของการสร้างความร่วมมือ
- 2) ดำเนินการจัดทำ MOU กับองค์กรเป้าหมาย เพื่อยกระดับความเชี่ยวชาญเฉพาะด้าน เช่น ร่วมมือกับบริษัท Cybersecurity เพื่ออบรมเจ้าหน้าที่ ร่วมสร้างแผน Cybersecurity หรือทดสอบระบบ (penetration test)
- 3) จัดกิจกรรมร่วมกับพันธมิตรที่ช่วยให้นักศึกษาและบุคลากรเข้าถึงเทคโนโลยีใหม่ ๆ เช่น Testbed Sandbox, เวิร์กช็อปเทคโนโลยี AI หรือ Cloud, หรือกิจกรรม Tech Talk ร่วมกับผู้เชี่ยวชาญจากภายนอก

- 4) ร่วมพัฒนาแพลตฟอร์ม/บริการดิจิทัลที่ใช้งานจริงในมหาวิทยาลัย เช่น ระบบแจ้งเตือนอัจฉริยะ, Dashboard สำหรับผู้บริหาร, หรือแอปพลิเคชันนักศึกษา โดยใช้เทคโนโลยีที่ภาคีถ่ายทอดให้
- 5) พัฒนาระบบติดตามผลความร่วมมือ (Partnership Monitoring System) เพื่อตรวจสอบว่าแต่ละความร่วมมือมีความคืบหน้า มีผลผลิต (output) และผลลัพธ์ (outcome) ต่อการเป็น Digital University หรือไม่ เช่น จำนวนบริการใหม่ จำนวนคนเข้าร่วมอบรม หรือระบบที่ถูกใช้งานจริง

ตารางที่ 19 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Ecosystem & Collaboration
มหาวิทยาลัย 4.0 (อว.)	Community Engagement, Regional Innovation
Digital Economy Plan	Digital Innovation Platform, Open Collaboration

ตารางที่ 20 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 7

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	จำนวนความร่วมมือด้านดิจิทัลกับองค์กรภายนอก	≥ 10 แห่ง	องค์กร	เช่น MOU กับบริษัท IT, หน่วยงานรัฐ, มหาวิทยาลัยอื่น
2	จำนวนโครงการนวัตกรรมดิจิทัลที่ดำเนินการจริง	≥ 5 โครงการ/ปี	โครงการ	พัฒนาโดยนักศึกษา/บุคลากร เช่น แอปพลิเคชัน แพลตฟอร์ม
3	จำนวนกิจกรรมส่งเสริมนวัตกรรมหรือ Tech Showcase	≥ 4 ครั้ง/ปี	กิจกรรม	เช่น Hackathon, Startup Pitching, Tech Day
4	จำนวนนักศึกษา/บุคลากรที่ได้รับทุนหรือรางวัลจากโครงการนวัตกรรม	≥ 20 คน/ปี	คน	เช่น ทุน DEPA, การแข่งขันระดับชาติ
5	สัดส่วนความร่วมมือที่มีผลต่อการพัฒนาศักยภาพภายในมหาวิทยาลัย	≥ 50%	ร้อยละของความร่วมมือ	เช่น ความร่วมมือที่นำไปสู่การใช้ระบบใหม่, การอบรมเทคโนโลยี, Co-Development

องค์ประกอบนี้มุ่งเน้นการสร้างระบบนิเวศดิจิทัล (Digital Ecosystem) ที่เชื่อมโยงมหาวิทยาลัยกับองค์กรภายนอก เพื่อเสริมสร้างศักยภาพและเร่งการเปลี่ยนผ่านสู่ Digital University ได้อย่างยั่งยืน ความร่วมมือในลักษณะนี้อาจครอบคลุมการพัฒนาระบบ เทคโนโลยี การเรียนรู้ร่วมกัน หรือการสร้างนวัตกรรมใหม่ๆ ตัวชี้วัดในองค์ประกอบนี้สะท้อนถึงความกว้าง ความลึก และผลลัพธ์ที่เกิดขึ้นจากความร่วมมือ โดยมีรายละเอียดดังนี้

KPI 1: จำนวนความร่วมมือด้านดิจิทัลกับองค์กรภายนอก วัดจากจำนวนหน่วยงานหรือองค์กรที่มหาวิทยาลัยมีความร่วมมือด้านดิจิทัล ไม่ว่าจะเป็นการลงนาม MOU, MOA หรือการร่วมดำเนินโครงการ เช่น ร่วมกับบริษัท Cloud พัฒนาระบบ, หน่วยงานรัฐร่วมอบรม PDPA หรือบริษัทรักษาความปลอดภัยทางไซเบอร์

KPI 2: จำนวนโครงการนวัตกรรมดิจิทัลที่ดำเนินการจริง วัดจากจำนวนโครงการที่ถูกออกแบบและใช้งานจริง ไม่ใช่แค่แนวคิด เช่น ระบบแจ้งเตือนผ่าน LINE, Dashboard การบริหารเวลาเรียน, หรือแอปพลิเคชันพัฒนาร่วมกับภาคีภายนอกโดยนักศึกษาและอาจารย์

KPI 4: จำนวนกิจกรรมส่งเสริมนวัตกรรมหรือ Tech Showcase วัดจากกิจกรรมที่เปิดโอกาสให้นักศึกษาและบุคลากรแสดงไอเดียและนวัตกรรม เช่น Hackathon, VRU Tech Day, การแข่งขันโค้ด หรือการนำเสนอระบบต้นแบบที่สร้างโดยชาวมหาวิทยาลัย

KPI 5: จำนวนนักศึกษา/บุคลากรที่ได้รับทุนหรือรางวัลจากโครงการนวัตกรรม วัดจากจำนวนคนที่ได้รับการสนับสนุน เช่น ทุนจากโครงการหน่วยงานภายนอก (เช่น depa, SIPA, โครงการ Startup Thailand) หรือการแข่งขันที่เกี่ยวข้องกับนวัตกรรมดิจิทัล

KPI 6: สัดส่วนความร่วมมือที่มีผลต่อการพัฒนาศักยภาพภายในมหาวิทยาลัย วัดจากสัดส่วนความร่วมมือที่ส่งผลต่อการยกระดับระบบ กระบวนการ หรือบุคลากรในมหาวิทยาลัย เช่น ร่วมพัฒนาระบบ SSO, จัดอบรมพิเศษเฉพาะบุคลากร หรือใช้ระบบ Sandbox ทดลองเทคโนโลยีใหม่

5.5.5 องค์ประกอบที่ 5: People & Digital Culture (PDC)

เทคโนโลยีที่ล้ำสมัยหรือระบบดิจิทัลที่ถูกออกแบบมาอย่างดีเพียงใด ก็ไม่อาจประสบผลสำเร็จได้ หากบุคลากรภายในองค์กรขาดความเข้าใจ ขาดทักษะ หรือขาดทัศนคติที่เปิดรับต่อการเปลี่ยนแปลง

People & Digital Culture จึงถือเป็น หัวใจด้านมนุษย์ ของกรอบการทำงานVRU-DUF โดยเน้นการพัฒนาศักยภาพคนในองค์กรให้สามารถอยู่ร่วมกับเทคโนโลยีอย่างมีความสุข พร้อมทั้งสร้างวัฒนธรรมองค์กรที่เอื้อต่อการเรียนรู้ การทดลอง และการปรับตัวอย่างต่อเนื่อง

■ เป้าหมายหลัก

- 1) ยกระดับทักษะดิจิทัลของบุคลากรและนักศึกษาให้สามารถใช้เครื่องมือดิจิทัลได้อย่างมีประสิทธิภาพ
- 2) สร้างวัฒนธรรมองค์กรที่ส่งเสริมการเปลี่ยนผ่านดิจิทัล
- 3) ปลูกฝังแนวคิด Digital Mindset ในทุกระดับขององค์กร

■ แนวทางการดำเนินงาน

- 1) จัดทำแผนพัฒนาทักษะดิจิทัล (Digital Competency Development Plan) ครอบคลุมตั้งแต่ระดับพื้นฐาน (Digital Literacy) จนถึงระดับเชี่ยวชาญ (AI, Data Analytics, Coding)
- 2) จัดอบรมและ Upskill / Reskill อย่างต่อเนื่อง ผ่านช่องทางที่หลากหลาย เช่น หลักสูตรออนไลน์, ห้องเรียนดิจิทัล, การเรียนรู้แบบ Microlearning
- 3) ตั้งเครือข่าย Digital Ambassador ประจำหน่วยงาน/คณะ ทำหน้าที่เป็นตัวแทนเชื่อมโยงและช่วยสนับสนุนการเปลี่ยนผ่านในแต่ละพื้นที่
- 4) จัดกิจกรรมส่งเสริมวัฒนธรรมดิจิทัล เช่น Hackathon, VRU Digital Week, กิจกรรม Challenge ด้านดิจิทัลที่มีการให้รางวัล/ยกย่อง
- 5) ใช้แนวคิด Learning Organization ส่งเสริมการเรียนรู้แบบข้ามสายงาน การแลกเปลี่ยนความรู้ และการใช้แพลตฟอร์มร่วมกัน

ตารางที่ 13 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Digital Workforce, Change Management
มหาวิทยาลัย 4.0 (อว.)	Digital Mindset, Lifelong Learning
NIST CSF 2.0	Govern / Protect (การให้สิทธิ์และอบรมผู้ใช้ระบบ)

ตารางที่ 14 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 4

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	สัดส่วนบุคลากรที่ผ่านการอบรม Digital Literacy	≥ 70%	ร้อยละของบุคลากร	วัดจากรายชื่อผู้ผ่านการอบรมที่จัดโดยมหาวิทยาลัย

2	จำนวนหลักสูตรอบรมที่เกี่ยวข้องกับทักษะดิจิทัล	≥ 10 หลักสูตร	หลักสูตร	รวมทั้งอบรมภายใน, e-Learning และกิจกรรมร่วมภายนอก
3	จำนวน Digital Ambassadors ที่ได้รับแต่งตั้ง	≥ 1 คน/หน่วยงาน	คน	ทำหน้าที่ประสานการเปลี่ยนผ่านดิจิทัลในระดับหน่วยงาน
4	จำนวนกิจกรรมส่งเสริมวัฒนธรรมดิจิทัล (Digital Culture Events)	≥ 4 ครั้ง/ปี	กิจกรรม	เช่น Hackathon, VRU Digital Week, Digital Challenge
5	ระดับความตระหนักรู้ของบุคลากรต่อการเปลี่ยนผ่านสู่ดิจิทัล	≥ 4.0	คะแนนเฉลี่ย	วัดจากแบบสอบถามหลังอบรมหรือแบบประเมินรายปี
6	สัดส่วนคณะ/สำนักที่มีแผนพัฒนาทักษะดิจิทัลเฉพาะของตนเอง	≥ 80%	ร้อยละของหน่วยงาน	วัดจากแผนพัฒนาบุคลากรรายปีของแต่ละหน่วย

การเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัลไม่สามารถเกิดขึ้นได้เพียงแค่มีระบบและเทคโนโลยีที่ดี แต่ต้องมีกำลังคนที่ เข้าใจ และ ปรับตัว ไปกับการเปลี่ยนแปลงทางดิจิทัลอย่างมีวัฒนธรรมร่วม องค์กรประกอบนี้จึงมุ่งวัดความพร้อมด้านทักษะ ความเข้าใจ และการส่งเสริมวัฒนธรรมดิจิทัลของบุคลากรทั้งระบบ โดยตัวชี้วัดประกอบด้วย:

KPI 1: สัดส่วนบุคลากรที่ผ่านการอบรม Digital Literacy วัดจำนวนบุคลากรที่เข้าร่วมและผ่านการอบรมในหลักสูตรที่เกี่ยวข้องกับการใช้งานเทคโนโลยีพื้นฐาน เช่น Microsoft 365, การใช้งาน LMS, ความปลอดภัยไซเบอร์ หรือ AI เพื่อการทำงาน

KPI 2: จำนวนหลักสูตรอบรมที่เกี่ยวข้องกับทักษะดิจิทัล วัดจากจำนวนหลักสูตรที่จัดทั้งในรูปแบบอบรมภายในมหาวิทยาลัย, ร่วมกับหน่วยงานภายนอก หรือ e-Learning ที่เน้นการเสริมทักษะ เช่น Data Analysis, Design Thinking, Coding เบื้องต้น ฯลฯ

KPI 3: จำนวน Digital Ambassadors ที่ได้รับแต่งตั้ง วัดจำนวนบุคลากรที่แต่ละหน่วยงานแต่งตั้งให้เป็นตัวกลางประสานการนำเทคโนโลยีใหม่ ๆ เข้าสู่หน่วยงาน เช่น ช่วยแนะนำการใช้ระบบใหม่ ประสานกับศูนย์ไอที และส่งต่อข้อมูลการอบรม

KPI 4: จำนวนกิจกรรมส่งเสริมวัฒนธรรมดิจิทัล (Digital Culture Events) วัดจากกิจกรรมที่ช่วยสร้างการมีส่วนร่วม ความเข้าใจ และแรงบันดาลใจด้านดิจิทัล เช่น Hackathon, VRU Digital Week, การประกวดไอเดีย หรือกิจกรรมแนะนำ AI/Tech ให้กับบุคลากรและนักศึกษา

KPI 5: ระดับความตระหนักรู้ของบุคลากรต่อการเปลี่ยนผ่านสู่ดิจิทัล วัดจากแบบสอบถามหลังอบรมหรือแบบประเมินรายปี เช่น ความเข้าใจเกี่ยวกับแผนดิจิทัล ความเชื่อมั่นในการใช้เทคโนโลยี หรือมุมมองต่อการเปลี่ยนแปลงองค์กร

KPI 6: สัดส่วนคณะ/สำนักที่มีแผนพัฒนาทักษะดิจิทัลเฉพาะของตนเอง วัดจำนวนหน่วยงานที่จัดทำแผนพัฒนาทักษะบุคลากรด้านดิจิทัลให้เหมาะสมกับบทบาทงานของตนเอง เช่น สำนักทะเบียนเน้นระบบจัดการข้อมูล, คณะศึกษาศาสตร์เน้น EdTech ฯลฯ

5.5.6 องค์กรประกอบที่ 6: Data Governance & Intelligence (DGI)

ในยุคที่ข้อมูลเป็นทรัพยากรสำคัญของการบริหารจัดการ การตัดสินใจ และการพัฒนานวัตกรรม การมีระบบจัดการข้อมูลที่เป็นระบบ โปร่งใส และปลอดภัย จึงกลายเป็นปัจจัยสำคัญของ มหาวิทยาลัยดิจิทัลอย่างหลีกเลี่ยงไม่ได้

Data Governance & Intelligence คือกระบวนการบริหารจัดการข้อมูล (Data Governance) ควบคู่กับการใช้ข้อมูลอย่างชาญฉลาด (Data Intelligence) เพื่อสร้างความสามารถในการวิเคราะห์ ตัดสินใจ และพัฒนาคุณภาพการบริหารและการเรียนรู้

■ เป้าหมายหลัก

- 1) มีการจัดโครงสร้างข้อมูลอย่างเป็นระบบ และสามารถบูรณาการข้อมูลจากหลายหน่วยงานได้
- 2) สร้างระบบข้อมูลกลางที่รองรับการใช้งานของผู้บริหาร อาจารย์ บุคลากร และนักศึกษา
- 3) พัฒนาการใช้ข้อมูลเพื่อการวิเคราะห์ (Analytics) และการพยากรณ์ (Prediction)
- 4) รักษาความถูกต้อง ปลอดภัย และความเป็นส่วนตัวของข้อมูล

■ แนวทางการดำเนินงาน

- 1) กำหนด เจ้าของข้อมูล (Data Owner) และผู้ดูแล (Data Steward) เพื่อสร้างความรับผิดชอบชัดเจนในแต่ละชุดข้อมูล เช่น ข้อมูลนักศึกษา, บุคลากร, วิจัย
- 2) จัดทำ Metadata และ Data Dictionary กลาง เพื่อกำหนดนิยาม ขอบเขต และโครงสร้างของข้อมูลให้ใช้ร่วมกันได้ทั้งองค์กร
- 3) พัฒนา Data Lake หรือ Data Warehouse ของมหาวิทยาลัย สำหรับรวมข้อมูลจากหลายระบบ เช่น ทะเบียน นักศึกษา การเงิน HR e-Document ฯลฯ
- 4) สร้าง Dashboard สำหรับผู้บริหารและหน่วยงาน เช่น Dashboard นักศึกษาเข้า-ออก, การใช้ทรัพยากร, ตัวชี้วัดระดับหลักสูตร
- 5) นำเทคโนโลยี AI / BI / Big Data Analytics มาใช้ในกระบวนการตัดสินใจ เช่น ระบบ Early Warning นักศึกษาตกหล่น, การวางแผนสอน, ประสิทธิภาพงบประมาณ

ตารางที่ 15 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Data Governance, Data Analytics
มหาวิทยาลัย 4.0 (อว.)	Data-driven Management
NIST CSF 2.0	Identify / Protect (การระบุข้อมูลสำคัญและการควบคุมสิทธิ์)

ตารางที่ 16 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 5

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	จำนวนชุดข้อมูลหลัก (Master Data Set) ที่มีการระบุเจ้าของข้อมูลอย่างชัดเจน	≥ 10 ชุด	ชุดข้อมูล	เช่น ข้อมูลนักศึกษา บุคลากร หลักสูตร งบประมาณ ฯลฯ
2	จำนวน Dashboard ที่พัฒนาขึ้นเพื่อสนับสนุนการบริหารจัดการ	≥ 5 รายการ	Dashboard	เช่น Dashboard นักศึกษาเข้าออก, การใช้งบประมาณ, ภาระงาน
3	การจัดทำ Metadata และ Data Dictionary กลาง	ต้องมี	มี/ไม่มี	ใช้กำหนดโครงสร้างและคำนิยามข้อมูลที่ใช้ร่วมกัน
4	ความพร้อมของระบบจัดเก็บข้อมูลกลาง (Data Lake หรือ Data Warehouse)	≥ 1 ระบบ	ระบบ	ต้องสามารถดึงข้อมูลจากหลายแหล่งและมีความปลอดภัย
5	สัดส่วนหน่วยงานที่ใช้ข้อมูลประกอบการตัดสินใจ	≥ 70%	ร้อยละของหน่วยงาน	วัดจากรายงานหรือกรณีใช้งานจริง เช่น ใช้ในการวางแผนสอน หรือจัดคนเข้าทำงาน

การเป็นมหาวิทยาลัยดิจิทัลต้องมี ข้อมูล ที่เชื่อถือได้ เป็นระบบ และนำไปใช้ในการตัดสินใจได้จริง องค์ประกอบนี้จึงมุ่งเน้นการสร้างวัฒนธรรมการใช้ข้อมูล (Data-Driven Culture) และการจัดการข้อมูลอย่างมีมาตรฐาน โดยแต่ละตัวชี้วัดสามารถอธิบายได้ดังนี้:

KPI 1: จำนวนชุดข้อมูลหลัก (Master Data Set) ที่มีการระบุเจ้าของข้อมูลอย่างชัดเจน วัดจำนวนชุดข้อมูลที่สำคัญ เช่น นักศึกษา, บุคลากร, หลักสูตร, งบประมาณ ฯลฯ ที่มีผู้รับผิดชอบชัดเจน (เช่น สำนักทะเบียน, กองคลัง) เพื่อลดความซ้ำซ้อนและป้องกันข้อมูลไม่ตรงกัน

KPI 2: จำนวน Dashboard ที่พัฒนาขึ้นเพื่อสนับสนุนการบริหารจัดการ วัดจากจำนวนแดชบอร์ดที่ช่วยให้ผู้บริหารและหน่วยงานตัดสินใจได้ง่ายขึ้น เช่น Dashboard การเข้าเรียน, สถิติการใช้จ่าย, ภาระงานอาจารย์ ซึ่งควรอัปเดตข้อมูลแบบ Real-time หรือรายสัปดาห์

KPI 3: การจัดทำ Metadata และ Data Dictionary กลาง วัดจากการจัดทำเอกสารหรือระบบที่อธิบายว่า ข้อมูลแต่ละฟิลด์หมายถึงอะไร เช่น คำว่า GPA หมายถึงอะไร หน่วยเป็นอะไร เก็บจากระบบไหน เพื่อให้การสื่อสารระหว่างหน่วยงานมีความเข้าใจตรงกัน

KPI 4: ความพร้อมของระบบจัดเก็บข้อมูลกลาง (Data Lake หรือ Data Warehouse) วัดจากการมีระบบที่สามารถรวบรวมข้อมูลจากหลายระบบ เช่น จาก Reg, HR, Finance มาไว้ที่เดียว และสามารถเรียกใช้ได้อย่างปลอดภัย เช่น ระบบ Data Lake บน Cloud ที่มีสิทธิ์การเข้าถึงแบบ Role-Based

KPI 5: สัดส่วนหน่วยงานที่ใช้ข้อมูลประกอบการตัดสินใจ วัดจากจำนวนหน่วยงานที่อ้างอิงข้อมูลในการวางแผน เช่น การใช้ข้อมูลผลการเรียนเพื่อวางแผนสอน หรือการใช้สถิติงบประมาณเพื่อขออนุมัติโครงการ ซึ่งอาจประเมินจากรายงานหรือการสัมภาษณ์

5.5.7 องค์ประกอบที่ 7: Monitoring, Evaluation & Continuous Improvement (MECI)

การติดตามผล ประเมินผล และพัฒนาอย่างต่อเนื่อง ในยุคของการเปลี่ยนผ่านสู่มหาวิทยาลัยดิจิทัล การบริหารงานด้านเทคโนโลยีและนวัตกรรมไม่สามารถยึดติดกับแผนที่ตายตัวหรือดำเนินไปอย่างไร้การตรวจสอบได้ องค์ประกอบ MECI มีบทบาทสำคัญในฐานะ "กลไกควบคุมคุณภาพ" และ "ระบบป้อนกลับ" ที่ช่วยให้การดำเนินการในทุกด้านของ V-DUF สามารถถูกติดตาม ประเมิน และปรับปรุงได้ตลอดเวลา

เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอยู่เสมอ และความคาดหวังของผู้ใช้งาน (นักศึกษา, บุคลากร, ผู้บริหาร) ก็เปลี่ยนไปตามยุคสมัย มหาวิทยาลัยจึงต้องมีระบบที่สามารถ เรียนรู้จากข้อมูลจริง และใช้ผลลัพธ์เหล่านั้นมาปรับแผนหรือกลยุทธ์อย่างมีประสิทธิภาพ

■ เป้าหมายหลัก

- 1) มีระบบติดตามผลการดำเนินงานด้านดิจิทัลอย่างเป็นระบบและต่อเนื่อง
- 2) สามารถประเมินความก้าวหน้าและผลกระทบของแผนดิจิทัลได้ในทั้งระดับโครงการและระดับองค์กร
- 3) มีระบบปรับปรุงแผนงานและกลยุทธ์ให้สอดคล้องกับบริบทที่เปลี่ยนแปลง
- 4) สร้างวัฒนธรรมองค์กรที่เน้นการเรียนรู้และพัฒนาอย่างไม่หยุดนิ่ง (Continuous Learning Culture)

■ แนวทางการดำเนินงาน

1) จัดทำ Digital KPI Dashboard สำหรับแต่ละหน่วยงาน พัฒนาระบบแสดงผลตัวชี้วัดดิจิทัลแบบ Real-Time โดยแสดงข้อมูลสำคัญ เช่น ร้อยละของบริการที่ให้แบบออนไลน์, ปริมาณการใช้งานแพลตฟอร์ม, ระยะเวลาเฉลี่ยในการให้บริการ และระดับความพึงพอใจของผู้ใช้งาน เพื่อให้ผู้บริหารสามารถติดตามผลการดำเนินงานของแต่ละหน่วยงานได้ทันทีและมีข้อมูลประกอบการตัดสินใจที่แม่นยำ

2) จัดประชุม V-DUF Progress Review เป็นรายเดือนหรือรายไตรมาส จัดเวทีติดตามผลการดำเนินงานของแผนดิจิทัล โดยให้แต่ละหน่วยงานรายงานความก้าวหน้า ปัญหา อุปสรรค และข้อเสนอแนะต่อคณะกรรมการกลาง เพื่อประเมินความคืบหน้าโดยรวม พร้อมทั้งเปิดโอกาสให้หน่วยงานแลกเปลี่ยนแนวปฏิบัติที่ดี (Best Practices)

3) ดำเนินการประเมินตนเอง (Self-Assessment) ด้วย Digital Maturity Model ใช้เครื่องมือประเมินระดับความพร้อมทางดิจิทัลของแต่ละหน่วยงาน เช่น แบบประเมินของ DGA หรือที่พัฒนาโดยมหาวิทยาลัยเอง โดยวัดในมิติต่าง ๆ เช่น โครงสร้างพื้นฐาน การบริหารข้อมูล การบริการดิจิทัล และวัฒนธรรมองค์กร เพื่อนำผลการประเมินไปวางแผนพัฒนาต่ออย่างเหมาะสม

4) ดำเนินการตรวจประเมินจากภายนอก (Audit หรือ External Evaluation) เชิญผู้เชี่ยวชาญหรือหน่วยงานภายนอกที่มีความน่าเชื่อถือเข้ามาประเมินความก้าวหน้าของการพัฒนาดิจิทัล เพื่อให้ได้มุมมองใหม่ที่เป็นกลาง เพิ่มความโปร่งใส และยกระดับมาตรฐานการพัฒนาให้เทียบเท่าสากล

5) จัดระบบรับฟังความคิดเห็นของผู้ใช้งาน (Feedback Loop) สร้างช่องทางรับฟังเสียงจากนักศึกษา บุคลากร และผู้ใช้งานระบบ ผ่านแบบสอบถามออนไลน์ การสัมภาษณ์เชิงลึก การสนทนากลุ่ม (Focus Group) หรือการติดตามความคิดเห็นจากโซเชียลมีเดีย (Social Listening) เพื่อให้การปรับปรุงระบบและบริการตอบสนองต่อความต้องการจริง

6) อัปเดตและปรับแผนดิจิทัลเป็นประจำ (Rolling Plan) ทบทวนและปรับปรุงแผนแม่บทดิจิทัล รวมถึงแผนปฏิบัติการรายปีอย่างต่อเนื่อง โดยพิจารณาจากผลประเมิน ความเปลี่ยนแปลงทางเทคโนโลยี และบริบทที่เปลี่ยนแปลง เพื่อไม่ให้แผนกลายเป็นเอกสารเชิงทฤษฎีที่ไม่มีการใช้งานจริง และรักษาความทันสมัยอยู่เสมอ

ตารางที่ 21 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA: Digital Government Framework	Performance Monitoring, Maturity Assessment – การติดตามผล และการประเมินความพร้อมดิจิทัล
มหาวิทยาลัย 4.0 (อว.)	Evaluation-Based Management – การบริหารจัดการบนพื้นฐานของผลการประเมินจริง
NIST CSF 2.0	Govern / Respond / Recover – การบริหารจัดการ ความพร้อมรับมือ และการฟื้นฟู โดยเน้นระบบรายงานผล (Monitoring & Reporting)

ตารางที่ 22 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 7

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	การจัดทำระบบ Dashboard เพื่อติดตามผลตัวชี้วัดด้านดิจิทัล	ต้องมี	มี / ไม่มี	ใช้แสดงผลตัวชี้วัด เช่น อัตราการใช้ระบบ, ความพึงพอใจ, ระยะเวลาบริการ
2	จำนวนครั้งของการจัดประชุมติดตามความคืบหน้า (Progress Review)	≥ 4 ครั้ง/ปี	ครั้ง	จัดโดยคณะกรรมการกลางหรืออนุกรรมการประจำองค์ประกอบ
3	จำนวนหน่วยงานที่ผ่านการประเมินตนเองด้วย Digital Maturity Model	≥ 80% ของหน่วยงาน	ร้อยละของหน่วยงาน	ใช้เครื่องมือจาก DGA, อว. หรือแบบประเมินที่พัฒนาเอง
4	จำนวนการประเมินจากภายนอกหรือการตรวจสอบคุณภาพระบบดิจิทัล (Audit)	≥ 1 ครั้ง/ปี	ครั้ง	ดำเนินการโดยผู้ประเมินอิสระหรือหน่วยงานภายนอกที่เกี่ยวข้อง
5	สัดส่วนหน่วยงานที่จัดทำแผนปรับปรุงหรือปรับแผนดิจิทัลตาม Feedback ที่ได้รับ	≥ 70% ของหน่วยงาน	ร้อยละของหน่วยงาน	วัดจากการตอบสนองต่อผลประเมิน, แบบสอบถาม, Social Listening
6	ความถี่ในการอัปเดตแผนดิจิทัลของมหาวิทยาลัย (Rolling Plan)	≥ 1 ครั้ง/ปี	ครั้ง	ต้องมีการปรับปรุงแผนตามสถานการณ์ที่เปลี่ยนแปลงทุกปี

องค์ประกอบนี้มุ่งเน้นการติดตาม ประเมินผล และปรับปรุงการดำเนินงานด้านดิจิทัลอย่างเป็นระบบ และต่อเนื่อง โดยมีเป้าหมายเพื่อให้มหาวิทยาลัยสามารถวัดผลลัพธ์จากแผนแม่บทดิจิทัลอย่างเป็นรูปธรรม เรียนรู้จากข้อมูลจริง และปรับกลยุทธ์ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงอยู่ตลอดเวลา องค์ประกอบนี้ยังช่วยส่งเสริมวัฒนธรรมขององค์กรที่ยึดหลักการเรียนรู้และพัฒนาอย่างต่อเนื่อง ตัวชี้วัดในองค์ประกอบนี้สะท้อนถึงความสามารถในการควบคุมคุณภาพและขับเคลื่อนการเปลี่ยนผ่านดิจิทัลอย่างมีประสิทธิภาพ ดังนี้

KPI 1: การจัดทำระบบ Dashboard เพื่อติดตามผลตัวชี้วัดด้านดิจิทัล วัดจากการมีอยู่ของ Dashboard กลางที่สามารถสรุปตัวชี้วัดด้านดิจิทัลของแต่ละหน่วยงาน เช่น ร้อยละของบริการที่ออนไลน์, จำนวนผู้ใช้งานระบบ, ระยะเวลาการให้บริการเฉลี่ย หรือระดับความพึงพอใจของผู้ใช้ โดยระบบนี้ต้องใช้งานได้จริงและเป็นเครื่องมือประกอบการตัดสินใจเชิงบริหาร

KPI 2: จำนวนครั้งของการจัดประชุมติดตามความคืบหน้า (Progress Review) วัดจากจำนวนครั้งที่จัดประชุมของคณะทำงานหรือคณะกรรมการที่เกี่ยวข้อง เพื่อติดตามความคืบหน้าของแผนดิจิทัล พร้อมรายงานปัญหา อุปสรรค และข้อเสนอแนะแก่ผู้บริหาร โดยเน้นให้เกิดวัฒนธรรมการประเมินผลอย่างสม่ำเสมอ เช่น ทุกไตรมาส

KPI 3: จำนวนหน่วยงานที่ผ่านการประเมินตนเองด้วย Digital Maturity Model วัดจากร้อยละของหน่วยงานในมหาวิทยาลัยที่ดำเนินการประเมินตนเองด้านความพร้อมทางดิจิทัล โดยใช้เครื่องมือมาตรฐาน เช่น แบบประเมินของ DGA หรือแบบที่พัฒนาขึ้นเองในบริบทของมหาวิทยาลัย เพื่อให้แต่ละหน่วยสามารถวางแผนพัฒนาได้อย่างเหมาะสม

KPI 4: จำนวนการประเมินจากภายนอกหรือการตรวจสอบคุณภาพระบบดิจิทัล (Audit) วัดจากจำนวนครั้งที่มีการประเมินโครงการหรือระบบดิจิทัลโดยหน่วยงานภายนอก เช่น ผู้เชี่ยวชาญอิสระ หน่วยงานรัฐ หรือองค์กรพันธมิตร เพื่อเพิ่มความน่าเชื่อถือของผลประเมิน และเสริมสร้างมาตรฐานการพัฒนาให้เทียบเท่าสากล

KPI 5: สัดส่วนหน่วยงานที่จัดทำแผนปรับปรุงหรือปรับแผนดิจิทัลตาม Feedback ที่ได้รับ วัดจากจำนวนหน่วยงานที่มีการดำเนินการตอบสนองต่อผลการประเมินหรือข้อเสนอแนะ เช่น การปรับปรุงระบบที่มีปัญหา จัดอบรมเพิ่มเติม หรือเปลี่ยนแปลงแผนปฏิบัติงาน โดยอ้างอิงจากข้อมูลการประเมิน, แบบสอบถามผู้ใช้งาน, หรือผลการพึงเสียงจากช่องทางออนไลน์

KPI 6: ความถี่ในการอัปเดตแผนดิจิทัลของมหาวิทยาลัย (Rolling Plan) วัดจากจำนวนครั้งที่มีการทบทวนและปรับปรุงแผนแม่บทดิจิทัลหรือแผนรายปี เพื่อให้สอดคล้องกับสถานการณ์ปัจจุบัน เช่น การเปลี่ยนแปลงนโยบายภาครัฐ, เทคโนโลยีใหม่, หรือบริบทภายในองค์กร การอัปเดตนี้ต้องทำอย่างสม่ำเสมออย่างน้อยปีละครั้งเพื่อไม่ให้แผนกลายเป็นเอกสารล้าสมัย

5.5.8 องค์ประกอบที่ 8: Cybersecurity & Data Privacy (CDP)

ในโลกดิจิทัลที่ข้อมูลและระบบถูกใช้ในการบริหารงาน การเรียนรู้ และการวิจัยอย่างเข้มข้นมากขึ้น ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) และการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) จึงกลายเป็นเงื่อนไขจำเป็น ที่มหาวิทยาลัยไม่สามารถมองข้ามได้

Cybersecurity & Data Privacy เป็นองค์ประกอบที่เน้นการปกป้องโครงสร้างพื้นฐานดิจิทัลของมหาวิทยาลัยจากภัยคุกคาม รวมถึงการจัดการข้อมูลของนักศึกษา บุคลากร และผู้มีส่วนเกี่ยวข้องอย่างรอบคอบ โดยยึดตามมาตรฐานและกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และแนวทางของ NIST Cybersecurity Framework (CSF) 2.0

- เป้าหมายหลัก

- 1) มีระบบและมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็ง
- 2) คุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย PDPA อย่างเป็นระบบ
- 3) มีความพร้อมในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติด้าน IT
- 4) ส่งเสริมความตระหนักรู้ด้านความปลอดภัยให้แก่บุคลากรและนักศึกษา

■ แนวทางการดำเนินงาน

- 1) นำ NIST CSF 2.0 มาใช้ในการวางระบบความมั่นคงปลอดภัยครอบคลุม 6 ฟังก์ชัน: Govern, Identify, Protect, Detect, Respond, Recover พร้อมกำหนด Tier และแผนพัฒนา
- 2) จัดตั้งหน่วยงานรับผิดชอบด้านความปลอดภัยไซเบอร์ (CSIRT) ทำหน้าที่ตรวจสอบ แจ้งเตือน และรับมือกับเหตุการณ์ด้านไซเบอร์
- 3) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) พร้อมจัดทำนโยบาย PDPA, แบบฟอร์มขอความยินยอม, ระบบการขอใช้สิทธิ์ของเจ้าของข้อมูล
- 4) ติดตั้งเครื่องมือป้องกันภัยคุกคาม (Firewall, Antivirus, SIEM, MFA) และวางระบบสำรองข้อมูล (Backup) และระบบ DR Site
- 5) จัดอบรมสร้างความตระหนักรู้ด้าน Cybersecurity และ PDPA ให้แก่บุคลากร นักศึกษา และผู้ใช้งานระบบต่าง ๆ ของมหาวิทยาลัย

ตารางที่ 17 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
NIST CSF 2.0	ครบทั้ง 6 ฟังก์ชัน: Govern, Identify, Protect, Detect, Respond, Recover
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)	DPO, Consent, Data Subject Rights, Privacy Policy
พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์	CSIRT, Notification, Risk Management
DGA Digital Government	Security & Privacy Standards, IT Audit

ตารางที่ 18 แสดงแผนผังตัวชี้วัดผลการดำเนินงาน องค์ที่ 6

ลำดับ	ตัวชี้วัด	เป้าหมาย	หน่วยวัด	หมายเหตุ
1	การจัดทำแผนบริหารความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Plan)	ต้องมี	มี/ไม่มี	ครอบคลุมนโยบาย มาตรการ และการตอบสนองเหตุการณ์
2	สัดส่วนระบบสารสนเทศที่มีการประเมินความเสี่ยงด้านไซเบอร์	≥ 100%	ร้อยละของระบบ	ทุกระบบต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง
3	การแต่งตั้งคณะกรรมการหรือ CSIRT (Computer Security Incident Response Team)	ต้องมี	มี/ไม่มี	เพื่อรับมือเมื่อเกิดเหตุผิดปกติ เช่น ข้อมูลรั่วไหล ระบบล่ม
4	สัดส่วนบุคลากรที่ผ่านการอบรม PDPA/ความมั่นคงไซเบอร์	≥ 80%	ร้อยละของบุคลากร	ครอบคลุมบุคลากรสายวิชาการ และสายสนับสนุน
5	จำนวนเหตุการณ์ด้านความปลอดภัยที่ตรวจพบและจัดการได้ทันเวลา	≥ 95%	ร้อยละของเหตุการณ์	วัดการตอบสนองและความพร้อมของระบบแจ้งเตือน
6	จำนวนระบบที่มีการควบคุมสิทธิการเข้าถึงตามหลัก Least Privilege	≥ 90%	ร้อยละของระบบ	ระบบสารสนเทศควรอนุญาตให้เข้าถึงเท่าที่จำเป็นเท่านั้น

ในโลกดิจิทัล ความปลอดภัยของข้อมูลและระบบเป็นหัวใจสำคัญที่ไม่สามารถมองข้ามได้ องค์ประกอบนี้เน้นการบริหารจัดการความเสี่ยงด้านไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อ

สร้างความเชื่อมั่นให้กับผู้ใช้ ทั้งนักศึกษา บุคลากร และพันธมิตร ตัวชี้วัดแต่ละข้อนี้ออกแบบมาเพื่อให้ครอบคลุมทั้งเชิง นโยบาย-ระบบ-คน ดังนี้:

KPI 1: การจัดทำแผนบริหารความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Plan) วัดจากการมีเอกสารแผนอย่างเป็นทางการ ซึ่งครอบคลุมนโยบายการใช้งาน ระบบควบคุมความปลอดภัย และแผนตอบสนองเหตุการณ์ เช่น แผนรับมือเมื่อระบบถูกโจมตีทางไซเบอร์

KPI 2: สัดส่วนระบบสารสนเทศที่มีการประเมินความเสี่ยงด้านไซเบอร์ ทุกระบบ เช่น ระบบเกรด ระบบบุคลากร ระบบการเงิน ควรได้รับการประเมินความเสี่ยงเป็นประจำ เช่น ตรวจสอบช่องโหว่ การตั้งค่าที่ผิดปกติ หรือจุดเสี่ยงที่อาจทำให้ข้อมูลรั่วไหล

KPI 3: การแต่งตั้งคณะกรรมการหรือ CSIRT (Computer Security Incident Response Team) หมายถึงการมีทีมเฉพาะรับมือเหตุการณ์ผิดปกติ เช่น ถูกแฮก ข้อมูลหาย หรือระบบล่ม โดยทีมนี้ต้องมีบทบาทหน้าที่ชัดเจนและสามารถปฏิบัติการได้จริง

KPI 4: สัดส่วนบุคลากรที่ผ่านการอบรม PDPA/ความมั่นคงไซเบอร์ วัดจากจำนวนบุคลากรที่เข้าอบรม เช่น เรื่องการปกป้องข้อมูลนักศึกษา การใช้รหัสผ่านอย่างปลอดภัย การรับมือ Phishing Email เป็นต้น โดยครอบคลุมทุกสายงาน

KPI 5: จำนวนเหตุการณ์ด้านความปลอดภัยที่ตรวจพบและจัดการได้ทันเวลา วัดจากประสิทธิภาพของระบบตรวจจับ เช่น ระบบแจ้งเตือนการเข้าใช้ระบบผิดปกติ และการตอบสนองของทีมเทคนิค เช่น เมื่อเกิดความผิดปกติ ระบบต้องส่งสัญญาณทันทีและมีการแก้ไขภายในเวลาที่กำหนด

KPI 6: จำนวนระบบที่มีการควบคุมสิทธิการเข้าถึงตามหลัก Least Privilege หมายถึงการให้สิทธิ์การใช้งานเฉพาะเท่าที่จำเป็น เช่น นักศึกษาจะเห็นเฉพาะข้อมูลตนเอง เจ้าหน้าที่ฝ่ายการเงินจะเข้าถึงเฉพาะระบบที่เกี่ยวข้องกับบัญชี ป้องกันความเสียหายจากการเข้าถึงโดยไม่ได้รับอนุญาต

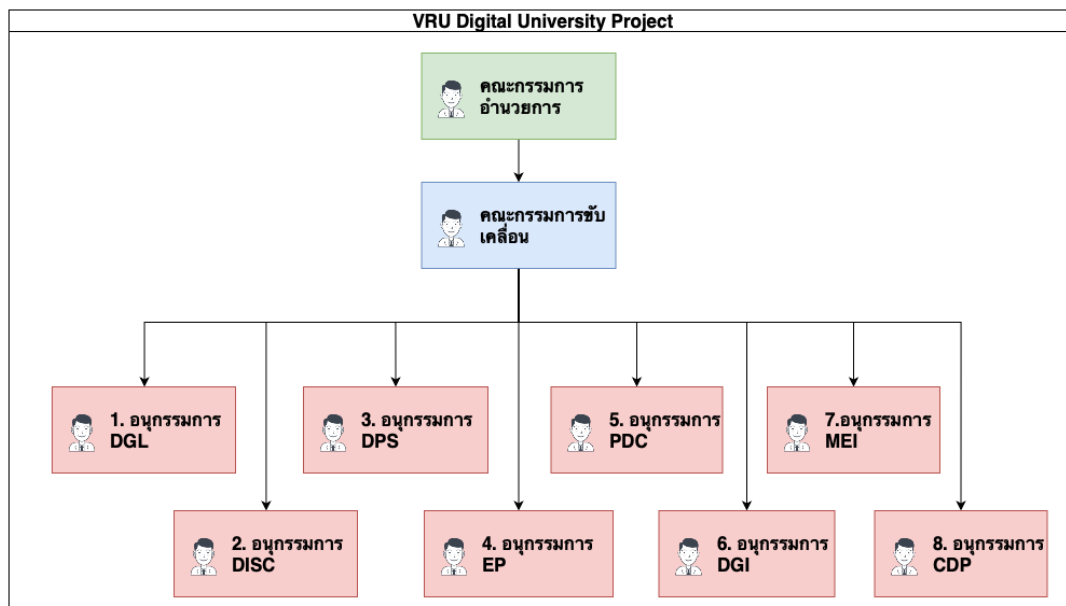
6. แผนขับเคลื่อนมหาวิทยาลัยดิจิทัล (Digital University Plan)

-

7. โครงสร้างการบริหาร V-DUF (VRU Digital University Framework)

เพื่อให้การดำเนินงานตามกรอบ V-DUF สามารถขับเคลื่อนได้อย่างมีประสิทธิภาพ ต่อเนื่อง และตรวจสอบได้อย่างเป็นระบบ มหาวิทยาลัยจำเป็นต้องมี โครงสร้างการบริหารจัดการเฉพาะด้าน ที่สามารถรองรับการเปลี่ยนแปลงทั้งเชิงนโยบาย เทคโนโลยี และการมีส่วนร่วมของทุกภาคส่วนในองค์กร

โครงสร้างนี้จึงถูกออกแบบในลักษณะสามระดับ ได้แก่ คณะกรรมการอำนวยการ คณะกรรมการขับเคลื่อน และอนุกรรมการเฉพาะด้านทั้ง 8 องค์กรประกอบตามกรอบ V-DUF เพื่อให้การบริหารสามารถกระจายอำนาจ กำหนดบทบาทอย่างชัดเจน และส่งเสริมการมีส่วนร่วมจากทุกหน่วยงานในมหาวิทยาลัย



รูปที่ 3 แสดงโครงสร้างการทำงาน

7.1. คณะกรรมการอำนวยการมหาวิทยาลัยดิจิทัล (Digital University Executive Board)

บทบาท: กำหนดนโยบาย วิสัยทัศน์ เป้าหมายสูงสุด อนุมัติแผนแม่บท และกำกับทิศทางรวมขององค์กร ประกอบด้วย:

- 1) อธิการบดี
- 2) รองอธิการบดี (Chief Information Officer: CIO)
- 3) ผู้ช่วยอธิการบดี (Chief Digital Officer: CDO)

7.2 คณะกรรมการขับเคลื่อน V-DUF (Digital Transformation Steering Committee)

บทบาท: วางแผนระดับยุทธศาสตร์ ออกแบบโครงการ กำกับติดตามการดำเนินงานรายเดือน รับรายงานจากอนุกรรมการทั้ง 8 ชุด

ประกอบด้วย:

- 1) CIO
- 2) CDO

7.3 อนุกรรมการเฉพาะด้าน (Sub-Committees for V-DUF Pillars)

ตั้ง 8 ชุด ตามองค์ประกอบ V-DUF พร้อมรายละเอียดหน้าที่และทีมงานแนะนำ:

▪ 1) อนุกรรมการ DGL (Governance & Leadership)

หน้าที่: กำหนดนโยบาย / ยุทธศาสตร์ดิจิทัล / ประเมินวิสัยทัศน์องค์กร

ประกอบด้วย:

- 1) CIO / CDO
- 2) ผอ.สำนักงานอธิการบดี / สำนักยุทธศาสตร์
- 3) หัวหน้าหน่วยงานวางแผน / QA
- 4) นักวิชาการวางแผน / กฎหมาย

▪ 2) อนุกรรมการ DISC (Infrastructure & Smart Campus)

หน้าที่: พัฒนา Network, Server, IoT, ระบบ Cloud และ Smart Facility

ประกอบด้วย:

- 1) CIO / CDO
- 2) หัวหน้าศูนย์คอมพิวเตอร์
- 3) วิศวกรเครือข่าย / นักคอมฯ ด้านโครงสร้างพื้นฐาน
- 4) หัวหน้าหน่วยอาคาร / สาธารณูปโภค
- 5) เจ้าหน้าที่ Smart Campus

▪ 3) อนุกรรมการ DPS (Platform & Services)

หน้าที่: พัฒนาแพลตฟอร์ม SSO, e-Service, Web Portal, e-Document

ประกอบด้วย:

- 1) CIO / CDO
- 2) หัวหน้าหน่วยงานทะเบียน, การเงิน, บุคลากร
- 3) นักพัฒนาระบบ / Full Stack / Laravel / Dev
- 4) ตัวแทนสายวิชาการผู้ใช้ระบบ
- 5) นักศึกษาตัวแทน / user tester

▪ 4) อนุกรรมการ EP (Ecosystem & Partnership)

หน้าที่: ประสานความร่วมมือ MOU, Sandbox, Open Innovation

ประกอบด้วย:

- 1) CIO / CDO
- 2) ผอ. สำนักวิจัย / สำนักพัฒนานักศึกษา
- 3) ตัวแทนหน่วยบ่มเพาะวิสาหกิจ / วิชาชีพ
- 4) นักวิจัย / อาจารย์กลุ่มบริการวิชาการ

เจ้าหน้าที่ความร่วมมือภายนอก

▪ 5) อนุกรรมการ PDC (People & Digital Culture)

หน้าที่: Upskill / Reskill บุคลากร, พัฒนา Digital Mindset และ Ambassadors

ประกอบด้วย:

- 1) CIO / CDO
- 2) ผอ. สำนักทรัพยากรบุคคล
- 3) หัวหน้าฝ่ายพัฒนาอาจารย์ / ฝึกอบรม
- 4) ตัวแทนคณะ / สาขาวิชา
- 5) นักวิชาการพัฒนาองค์กร

▪ 6) อนุกรรมการ DGI (Data Governance & Intelligence)

หน้าที่: จัดการ Master Data, Dashboard, Data Lake, วิเคราะห์ข้อมูล

ประกอบด้วย:

- 1) CIO / CDO
- 2) นักวิชาการคอมฯ ด้านข้อมูล
- 3) Data Owner จากหน่วยงานหลัก (ทะเบียน, HR, Finance)
- 4) เจ้าหน้าที่สารสนเทศ
- 5) นักวิเคราะห์ข้อมูล (BI / AI)

▪ 7) อนุกรรมการ MEI (Monitoring, Evaluation & Improvement)

หน้าที่: ติดตามผล, ประเมิน, จัดทำ Dashboard, สรุปบทเรียน

ประกอบด้วย:

- 1) CIO / CDO
- 2) นักวิชาการประกันคุณภาพ
- 3) เจ้าหน้าที่ฝ่ายแผน / สารสนเทศ
- 4) ตัวแทนแต่ละหน่วยรายงานผล
- 5) อาจารย์ด้าน Measurement / Evaluation

▪ 8) อนุกรรมการ CDP (Cybersecurity & Data Privacy)

หน้าที่: ดำเนินการด้าน NIST CSF, PDPA, ความมั่นคงปลอดภัยไซเบอร์

ประกอบด้วย:

- 1) CIO / CDO
- 2) DPO (เจ้าหน้าที่ PDPA)
- 3) หัวหน้าทีม CSIRT / Cyber Response
- 4) ตัวแทนฝ่ายกฎหมาย / นิติกร
- 5) นักคอมฯ ระบบและความปลอดภัย

8. สิ่งที่ได้จากอนุกรรมการ V-DUF ทั้ง 8 ชุด

อนุกรรมการ	สิ่งที่ต้องจัดทำ / ส่งมอบ (Deliverables)
1. DGL (Governance & Leadership)	- นโยบาย Digital Transformation - คำสั่งแต่งตั้งคณะกรรมการและ War Room - แผนแม่บท V-DUF (Master Plan) - Digital KPI รายงานหน่วยงาน
2. DISC (Infrastructure & Smart Campus)	- แผนผังเครือข่าย / โครงสร้างพื้นฐานใหม่ - รายงานสถานะ Network, Server, IoT - แผนจัดซื้อ/อัปเกรดอุปกรณ์และระบบ - แผน Smart Campus (ในอนาคต)
3. DPS (Platform & Services)	- รายชื่อระบบ Platform ที่จะพัฒนา - ระบบต้นแบบ (Prototype): Portal, e-Document, SSO - แผนการเชื่อมระบบสารสนเทศ (Integration Plan) - คู่มือการใช้งานเบื้องต้น
4. EP (Ecosystem & Partnership)	- รายชื่อพันธมิตรหลักภายใน/ภายนอก - MOU ที่ลงนาม / ร่าง MOU - แผนพัฒนา Sandbox / Innovation Space - กิจกรรมความร่วมมือ / Hackathon / Co-research
5. PDC (People & Digital Culture)	- แผนพัฒนาทักษะบุคลากร (Digital Literacy / AI / BI) - ตารางอบรม, เอกสารประกอบการฝึกอบรม - รายชื่อ Digital Ambassador - แผนสร้างวัฒนธรรมดิจิทัลองค์กร

6. DGI (Data Governance & Intelligence)	- รายชื่อ Data Owner / Steward - Metadata / Data Dictionary (ฉบับแรก) - แผนพัฒนา Data Lake / Dashboard - ตัวอย่าง Dashboard สำหรับผู้บริหาร
7. MEI (Monitoring, Evaluation & Improvement)	- แผนการติดตามและประเมินผล V-DUF - Dashboard ติดตามผลรายองค์ประกอบ - รายงานความก้าวหน้า (รายเดือน/ไตรมาส) - สรุปบทเรียน / แผนปรับปรุงต่อเนื่อง (Rolling Plan)
8. CDP (Cybersecurity & Data Privacy)	- แต่งตั้ง DPO, ทีม CSIRT พร้อม TOR - นโยบาย PDPA และนโยบายความมั่นคงปลอดภัยไซเบอร์ - รายงานความเสี่ยง / แผนตอบสนองเหตุการณ์ (Incident Plan) - ผลการซ้อมระบบ / การอบรมด้านความปลอดภัย

9. เอกสารที่ใช้ในการดำเนินการในแต่ละองค์

องค์ประกอบ	รหัสเอกสาร	ชื่อเอกสาร	ประเภท	คำอธิบาย	เชื่อมโยงกับกิจกรรม
1. DGL	DGL-MP	แผนแม่บทมหาวิทยาลัยดิจิทัล	นโยบาย	แนวทางระดับยุทธศาสตร์ของการพัฒนา V-DUF	แผนยุทธศาสตร์/แผนหลัก
1. DGL	DGL-KPI	แผนตัวชี้วัดผลการดำเนินงาน	KPI	กำหนด KPI รายองค์ประกอบ เพื่อใช้ในการประเมินผล	ติดตามผลลัพธ์
1. DGL	DGL-Report	แบบรายงานความก้าวหน้าโครงการ	ภาคปฏิบัติ	รายงานความคืบหน้าการดำเนินงานประจำไตรมาส	การติดตามประจำไตรมาส
1. DGL	DGL-RiskMap	แผนภูมิความเสี่ยงด้านดิจิทัล	นโยบาย	ระบุความเสี่ยงหลักและแผนจัดการ	ความเสี่ยงองค์กร
1. DGL	DGL-CommPlan	แผนการสื่อสารผลการดำเนินงาน	นโยบาย	กำหนดวิธีการสื่อสารผลกับผู้เกี่ยวข้อง	Stakeholder Communication
2. DISC	DISC-NetworkPlan	แผนพัฒนาโครงข่ายพื้นฐาน	นโยบาย	วางแผนขยาย Wi-Fi, IoT, และระบบ Cloud	แผนพัฒนาโครงสร้างพื้นฐาน
2. DISC	DISC-InfraMap	แผนผังโครงสร้างระบบ	ภาคปฏิบัติ	แสดง topology และตำแหน่งอุปกรณ์	บริหารจัดการอุปกรณ์
2. DISC	DISC-BackupChecklist	แบบตรวจสอบระบบสำรองข้อมูล	Template	รายการตรวจสอบความพร้อม backup	ความต่อเนื่องทางธุรกิจ
2. DISC	DISC-CloudMigrationLog	บันทึกการย้ายระบบสู่ Cloud	ภาคปฏิบัติ	แสดงรายละเอียดระบบที่ย้าย	การเปลี่ยนผ่านสู่ดิจิทัล
3. DPS	DPS-Manual	คู่มือระบบบริการดิจิทัล	ภาคปฏิบัติ	วิธีใช้งาน Web Portal, SSO, Mobile App	การใช้งานระบบ
3. DPS	DPS-Feedback	รายงานความพึงพอใจ	KPI	สรุปผลจากแบบประเมินผู้ใช้งาน	การพัฒนาประสบการณ์ผู้ใช้
3. DPS	DPS-UXReport	รายงาน UX	วิเคราะห์	วิเคราะห์ประสบการณ์ผู้ใช้และข้อเสนอแนะ	ปรับปรุงการใช้งาน
3. DPS	DPS-MobileServiceLog	รายการบริการผ่าน Mobile/Web	ภาคปฏิบัติ	สรุปบริการที่พัฒนาแล้ว	การให้บริการ
5. PDC	PDC-TrainPlan	แผนการฝึกอบรมทักษะดิจิทัล	นโยบาย	กำหนดหลักสูตรและกลุ่มเป้าหมาย	เสริมสร้างศักยภาพ
5. PDC	PDC-CultureEvent	แผนกิจกรรมส่งเสริมวัฒนธรรมดิจิทัล	นโยบาย	ส่งเสริมบรรยากาศและทัศนคติดิจิทัล	วัฒนธรรมองค์กร
5. PDC	PDC-TrainRecord	บันทึกผู้เข้าอบรม	ภาคปฏิบัติ	เก็บข้อมูลบุคลากรที่เข้าร่วมกิจกรรม	หลักฐานการดำเนินการ
5. PDC	PDC-DigitalCultureSurvey	แบบประเมินวัฒนธรรมดิจิทัล	วิเคราะห์	วัดระดับความตระหนักรู้	การติดตามผลกิจกรรม
6. DGI	DGI-Dashboard	แบบฟอร์มสรุป Dashboard	ภาคปฏิบัติ	ตัวอย่าง Dashboard วิเคราะห์ข้อมูล	วิเคราะห์เชิงกลยุทธ์
6. DGI	DGI-DataDict	คู่มือ Metadata/Data Dictionary	Template	มาตรฐานการกำหนดชื่อและนิยามข้อมูล	การจัดการข้อมูล
6. DGI	DGI-UseCaseLog	บันทึกการใช้ข้อมูล (Use Case)	ภาคปฏิบัติ	รวบรวมกรณีการใช้ข้อมูลตัดสินใจ	การวิเคราะห์ข้อมูล
6. DGI	DGI-QualityAudit	รายงานตรวจสอบคุณภาพข้อมูล	วิเคราะห์	ประเมินคุณภาพข้อมูลที่ใช้งาน	Data Governance
6. CDP	CDP-IncidentPlan	แผนรับมือเหตุการณ์ไซเบอร์	นโยบาย	คู่มือและแนวทางตอบสนองกรณีฉุกเฉิน	Cybersecurity
6. CDP	CDP-Policy	นโยบายความปลอดภัยไซเบอร์	นโยบาย	ข้อกำหนดและมาตรการด้านความมั่นคง	PDPA & Cyber Policy
6. CDP	CDP-PDPARecord	บันทึกการอบรม PDPA	ภาคปฏิบัติ	เก็บข้อมูลผู้ผ่านการอบรม	PDPA Compliance
6. CDP	CDP-AuditTrailPolicy	นโยบายการจัดเก็บ Log	นโยบาย	แนวทางการจัดเก็บ/ตรวจสอบการใช้งานระบบ	Audit & Monitoring
7. AIN	AIN-Architecture	แผนภาพ Enterprise Architecture	Template	ความสัมพันธ์ระหว่างระบบทั้งหมด	System Integration
7. AIN	AIN-APIList	รายการ API ที่เชื่อมโยง	ภาคปฏิบัติ	รวม API และมาตรฐานการแลกเปลี่ยนข้อมูล	Interoperability
7. AIN	AIN-SSOMap	ผังระบบที่เข้าถึงผ่าน SSO	วิเคราะห์	ภาพรวมบริการที่เชื่อมกับ Single Sign-On	Authentication Framework

7. AIN	AIN-IntegrationProtocol	แนวทางการเชื่อมโยงระบบ	Template	รูปแบบมาตรฐาน JSON/XML	API & Protocol Design
8. IEP	IEP-InnovationReport	รายงานผลงานนวัตกรรม	ภาคปฏิบัติ	รวมโครงการ/ผลงานด้านนวัตกรรม	Tracking Innovation
8. IEP	IEP-TechShowcase	รายงานกิจกรรมเทคโนโลยี	ภาคปฏิบัติ	เช่น Hackathon, Demo Day	ประชาสัมพันธ์/เครือข่าย
8. IEP	IEP-PartnerMoU	สำเนาหรือทะเบียน MoU	ภาคปฏิบัติ	บันทึกความร่วมมือกับภาคี	Ecosystem & Partnership
8. IEP	IEP-ImpactReport	รายงานผลกระทบต่อชุมชน	วิเคราะห์	วัดผลจากนวัตกรรมต่อท้องถิ่น	Local Development

Version Control

หมายเลข	ความหมาย	ตัวอย่าง
V1.0	เวอร์ชันแรกที่เผยแพร่	DGL-KPI-V1.0
V1.1	แก้ไขเล็กน้อย (Minor Update)	เช่น เปลี่ยนชื่อหัวข้อ
V2.0	แก้ไขใหญ่ (Major Update)	เช่น เพิ่ม KPI ใหม่ เปลี่ยนโครงสร้าง
-2025	ระบุปี (ถ้าใช้แยกตามรอบงบประมาณหรือแผนปี)	IEP-InnovationReport-V1.0-2025

ตัวอย่าง รหัสเอกสาร

องค์ประกอบ	รูปแบบรหัสเอกสาร	ตัวอย่าง
1. DGL	DGL-MP-V1.0	แผนแม่บทเวอร์ชัน 1.0
4. DLC	PDC-TrainPlan-V2.1	แผนการอบรม เวอร์ชัน 2.1
6. CSP	CDP-IncidentPlan-V1.2-2025	แผนรับมือเหตุการณ์ไซเบอร์ เวอร์ชัน 1.2 ปี 2025

ปรับปรุงล่าสุด วันที่ 1 กรกฎาคม 2568
จัดทำโดย
ผู้ช่วยศาสตราจารย์ ดร.เศรษฐพงศ์ วงษ์อินทร์