



(ร่าง) แผนแม่บทมหาวิทยาลัยดิจิทัล มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์

1. ที่มาของแนวคิด Digital University ในประเทศไทย

ในช่วงทศวรรษที่ผ่านมา สังคมไทยได้เผชิญกับการเปลี่ยนแปลงอย่างรวดเร็วจากกระแสดิจิทัลทรานส์ฟอร์มเมชัน (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 ของมหาวิทยาลัยวลัยลักษณ์ (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 ตรวจสอบ และตอบสนองต่อภัยคุกคามทางไซเบอร์	- ตั้ง CSIRT (ทีมตอบสนองภัยไซเบอร์) - ทำแผนความปลอดภัยระบบสารสนเทศ - รายงานเหตุการณ์ผิดปกติ - ปฏิบัติตามแนวทาง NIST CSF 2.0
พ.ร.บ. จุฬารัฐธรรมนูญ 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 หรือแม้แต่การกำหนดโครงสร้างบุคลากรดิจิทัลภายในมหาวิทยาลัย

กฎหมายเหล่านี้อาจไม่ได้กล่าวถึงดิจิทัลอย่างตรงไปตรงมาในชื่อเรื่อง แต่กลับส่งผลอย่างมีนัยยะสำคัญต่อความถูกต้องตามระเบียบ และความคล่องตัวในการบริหารจัดการของมหาวิทยาลัย หากสามารถอ่านเกม และเชื่อมโยงกับแนวทางพัฒนา Digital University ได้อย่างเข้าใจ ก็จะช่วยลดข้อจำกัด และเปิดโอกาสให้การขับเคลื่อนนวัตกรรมภายในมหาวิทยาลัยได้อย่างยั่งยืน

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 อิงอ้างอิง

จากการวิเคราะห์นโยบายระดับชาติ กฎหมายที่เกี่ยวข้อง และกรอบการทำงานกลางที่หน่วยงานรัฐ และอุดมศึกษาใช้เป็นแนวทางในการพัฒนาดิจิทัล จะเห็นได้ว่าการพัฒนามหาวิทยาลัยดิจิทัล ไม่ได้เป็นเรื่องใหม่หรือแยกขาดจากระบบราชการไทย แต่เป็นกลยุทธ์ร่วมระดับประเทศ ที่มีหน่วยงานกำกับอย่างชัดเจน ทั้งในมิติดินโยบาย 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 DGA ที่เน้นการพัฒนาบริการอิเล็กทรอนิกส์ การเปิดเผยข้อมูล และความมั่นคงปลอดภัย

4.2 กรอบการทำงาน (Framework) ที่ควรใช้เป็นแนวอ้างอิง

กรอบการทำงานที่ควรใช้ในการออกแบบและวางระบบ Digital University มีดังนี้:

ตารางที่ 4 แสดงกฎหมายอื่น ๆ ที่เกี่ยวข้อง

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)

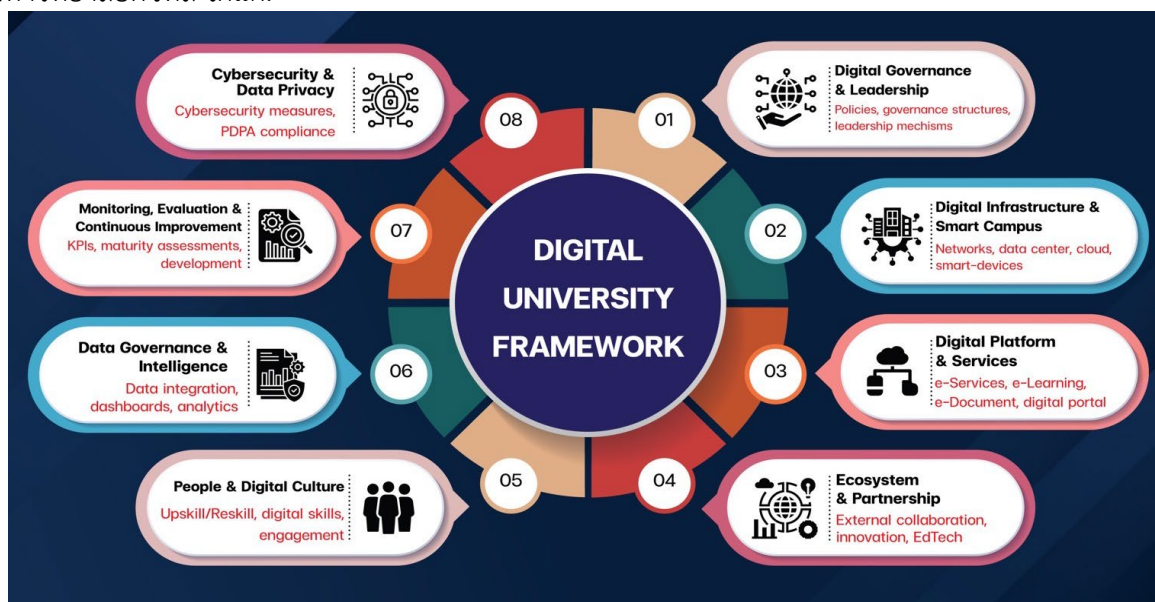
เมื่อแนวคิด Digital University กลายเป็นเป้าหมายเชิงยุทธศาสตร์ที่มหาวิทยาลัยทั่วประเทศต้องมุ่งสู่การดำเนินงานเพื่อไปถึงเป้าหมายนั้นจำเป็นต้องมีกรอบแนวทาง ที่ชัดเจน ครอบคลุม และสามารถวัดผลได้ กรอบการทำงานนี้ไม่ได้เป็นเพียงแค่โครงสร้างแนวคิดทางทฤษฎี แต่เป็นระบบคิดเชิงกลยุทธ์ ที่ช่วยให้องค์กรสามารถ:

- 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

กรอบการทำงาน V-DUF ประกอบด้วย 8 องค์ประกอบหลัก (8 Pillars) ซึ่งครอบคลุมการพัฒนาในทุกมิติของมหาวิทยาลัยดิจิทัล ได้แก่:



รูปที่ 1 แสดง VRU-DUF

ตารางที่ 5 แสดงองค์ประกอบทั้ง 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	People & Digital Culture (PDC)	การสร้างทักษะ ทักษะคน และวัฒนธรรมองค์กรให้พร้อมเข้าสู่ยุคดิจิทัล
5	Data Governance & Intelligence (DGI)	การบริหารข้อมูลอย่างเป็นระบบ รวมถึงการวิเคราะห์และใช้ข้อมูลในการตัดสินใจ
6	Cybersecurity & Data Privacy (CDP)	ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล (PDPA, NIST CSF)
7	Ecosystem & Partnership (EP)	การสร้างความร่วมมือกับภาครัฐ เอกชน และชุมชน เพื่อร่วมขับเคลื่อนดิจิทัล
8	Monitoring, Evaluation & Improvement (MEI)	การติดตามผล, ประเมินความก้าวหน้า และปรับปรุงอย่างต่อเนื่อง

5.2 การเชื่อมโยงกับมาตรฐาน / แนวนโยบายที่เกี่ยวข้อง

ในการพัฒนามหาวิทยาลัยดิจิทัลให้มีทิศทางที่ชัดเจน เป็นระบบ และสามารถตรวจสอบได้ จำเป็นอย่างยิ่งที่แผนงานจะต้องเชื่อมโยงกับ มาตรฐานกลางและนโยบายระดับชาติ ที่ได้รับการยอมรับ ทั้งในเชิงกฎหมาย มาตรฐานเทคโนโลยี และแนวปฏิบัติจากหน่วยงานกำกับดูแล เพื่อให้มั่นใจว่าการดำเนินงานมีความถูกต้อง ครบคลุม 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	ควรงอิง 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	☒ ตัวชี้วัดตามแผนระดับชาติ	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

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

Digital Governance & Leadership จึงถือเป็น หัวใจ ของกรอบการทำงานVRU-DUF ซึ่งจะทำให้หน้าที่กำหนดทิศทาง 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

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) มหาวิทยาลัยอาจแต่งตั้ง ผู้ช่วยอธิการบดีฝ่ายดิจิทัล หรือ CIO เพื่อทำหน้าที่กำกับยุทธศาสตร์อย่างต่อเนื่อง
- 2) ตั้งคณะทำงานเฉพาะกิจในระดับหน่วยงาน เช่น ทีมดิจิทัลคณะ/สำนัก ที่รายงานตรงต่อคณะกรรมการกลาง
- 3) นำแผนแม่บท VRU-DUF ไปจัดทำเป็น Roadmap รายปี พร้อมตัวชี้วัดรายเดือน/ไตรมาส

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)

5.5.2 องค์ประกอบที่ 2: Digital Infrastructure & Smart Campus

การพัฒนาระบบโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ 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) อัปเกรดระบบเครือข่าย (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

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) ปรับปรุงระบบ Wi-Fi ความเร็วสูงให้ครอบคลุมอาคารเรียนทุกคณะ
- 2) ใช้ระบบกล้องอัจฉริยะเชื่อมโยงกับ Dashboard ผู้บริหารด้านความปลอดภัย
- 3) จัดตั้ง Data Center กลาง เชื่อมโยงข้อมูลฝ่ายทะเบียน บริหารงานบุคคล และการเงิน
- 4) ใช้ Cloud ภาครัฐสำหรับระบบ e-Document และบริการนักศึกษา

ตารางที่ 8 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)

5.5.3 องค์ประกอบที่ 3: Digital Platform & Services

หลังจากวางโครงสร้างพื้นฐานทางดิจิทัล (Infrastructure) ได้อย่างมั่นคงแล้ว ขั้นตอนถัดมาที่จะทำให้ระบบดิจิทัลของมหาวิทยาลัย สามารถสัมผัสได้จริงโดยผู้ใช้งาน ได้แก่ การออกแบบและให้บริการผ่านแพลตฟอร์มดิจิทัล (Digital Platform) ซึ่งเป็นเครื่องมือหลักที่เชื่อมโยงผู้ใช้ บุคลากร นักศึกษา และระบบสนับสนุนทั้งหมดเข้าด้วยกัน

องค์ประกอบ Digital Platform & Services จึงเป็นเสมือน หน้าตา ของ Digital University โดยครอบคลุมทั้งระบบสารสนเทศพื้นฐาน งานบริการนักศึกษา ระบบสนับสนุนการเรียนการสอน การวิจัย และการบริหารจัดการภายใน

■ เป้าหมายหลัก

- 1) ให้บริการผ่านระบบดิจิทัลอย่างทั่วถึง ครอบคลุม และเข้าถึงได้ง่าย
- 2) ลดการใช้เอกสารแบบเดิม (paperless)
- 3) เชื่อมโยงข้อมูลระหว่างระบบเพื่อให้บริการแบบไร้รอยต่อ (Seamless Services)
- 4) ส่งเสริมการเรียนรู้และการบริหารงานที่ยืดหยุ่นผ่านเทคโนโลยี

■ แนวทางการดำเนินงาน

- 1) พัฒนาระบบ e-Document และ Workflow อิเล็กทรอนิกส์ เช่น ระบบหนังสือเวียน, ระบบขออนุมัติ, ระบบลาพักงาน/ขออนุ ฯลฯ ที่มีการลงนามดิจิทัลและสามารถตรวจสอบสถานะได้ตลอดเวลา
- 2) จัดตั้ง Web Portal กลางของมหาวิทยาลัย ให้เป็นศูนย์รวมการเข้าถึงระบบทั้งหมด เช่น ระบบทะเบียน, การเงิน, ประกันคุณภาพ, LMS, ห้องสมุด และ ChatGPT
- 3) เชื่อมโยงระบบผ่าน SSO (Single Sign-On) ผู้ใช้สามารถเข้าระบบทั้งหมดได้โดยใช้บัญชีเดียว เช่น E-mail มหาวิทยาลัย
- 4) ใช้ระบบ LMS และ Digital Classroom เช่น Google Classroom, Microsoft Teams, หรือระบบพัฒนาเอง ที่รองรับทั้ง synchronous และ asynchronous learning
- 5) ให้บริการ Mobile App / Chatbot / Kiosk เพื่อเพิ่มช่องทางการเข้าถึงบริการ และอำนวยความสะดวกให้กับนักศึกษาและบุคลากรในชีวิตประจำวัน

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) พัฒนาระบบ VRU Digital Portal สำหรับรวมลิงก์บริการดิจิทัลทั้งหมดไว้ในหน้าเดียว
- 2) ใช้ระบบ e-Office ที่มีฟังก์ชันตรวจสอบสถานะหนังสือออนไลน์ และสามารถลงนามดิจิทัลได้
- 3) เชื่อมต่อระบบทะเบียน (Reg), ห้องสมุด (Lib), การเงิน (Finance) และ LMS ผ่าน SSO
- 4) นำระบบ VRU Helpdesk Online มาใช้แทนการแจ้งงานแบบโทรศัพท์หรือกระดาษ

ตารางที่ 9 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)

5.5.4 องค์ประกอบที่ 4: People & Digital Culture

เทคโนโลยีที่ล้ำสมัยหรือระบบดิจิทัลที่ถูกออกแบบมาอย่างดีเพียงใด ก็ไม่อาจประสบความสำเร็จได้ หากบุคลากรภายในองค์กรขาดความเข้าใจ ขาดทักษะ หรือขาดทัศนคติที่เปิดรับการเปลี่ยนแปลง

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

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) พัฒนา หลักสูตรอบรม AI สำหรับบุคลากรสายสนับสนุน เพื่อสร้างความมั่นใจในการใช้เครื่องมืออัตโนมัติ เช่น ChatGPT หรือ Power Automate
- 2) แต่งตั้ง Digital Ambassador ประจำคณะ/สำนักงาน เช่น นักวิชาการคอมพิวเตอร์ หรือ บุคลากรเชิงรุก
- 3) จัดกิจกรรม VRU Digital Talk แลกเปลี่ยนแนวคิดและกรณีศึกษาจากหน่วยงานภายใน
- 4) บูรณาการหัวข้อ Digital Culture ลงในแผนพัฒนาบุคลากรรายปี

ตารางที่ 10 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)

5.5.5 องค์ประกอบที่ 5: Data Governance & Intelligence

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

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) แต่งตั้ง Data Steward ประจำระบบ เช่น ระบบทะเบียน, ระบบวิจัย, ระบบพัสดุ
- 2) จัดทำ VRU Data Lake เพื่อรวมข้อมูลจากฝ่ายทะเบียน การเงิน ห้องสมุด และประกันคุณภาพ
- 3) พัฒนา VRU Executive Dashboard ให้ผู้บริหารเห็นภาพรวมเชิงกลยุทธ์แบบเรียลไทม์
- 4) เชื่อมต่อข้อมูลจาก LMS กับผลการเรียน เพื่อประเมินการมีส่วนร่วมของนักศึกษาในรายวิชา

ตารางที่ 11 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

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

5.5.6 องค์ประกอบที่ 6: Cybersecurity & Data Privacy

ในโลกดิจิทัลที่ข้อมูลและระบบถูกใช้ในการบริหารงาน การเรียนรู้ และการวิจัยอย่างเข้มข้นมากขึ้น ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) และการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) จึงกลายเป็น เงื่อนไขจำเป็น 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 และ แผนพัฒนา
- 2) จัดตั้งหน่วยงานรับผิดชอบด้านความปลอดภัยไซเบอร์ (CSIRT) ทำหน้าที่ตรวจสอบ แจ้งเตือน และรับมือกับเหตุการณ์ด้านไซเบอร์
- 3) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) พร้อมจัดทำ นโยบาย PDPA, แบบฟอร์มขอความยินยอม, ระบบการขอใช้สิทธิ์ของเจ้าของข้อมูล
- 4) ติดตั้งเครื่องมือป้องกันภัยคุกคาม (Firewall, Antivirus, SIEM, MFA) และวางระบบสำรองข้อมูล (Backup) และระบบ DR Site
- 5) จัดอบรมสร้างความตระหนักรู้ด้าน Cybersecurity และ PDPA ให้แก่บุคลากร นักศึกษา และผู้ใช้งานระบบต่าง ๆ ของมหาวิทยาลัย

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) พัฒนา VRU Cybersecurity Policy และ Data Privacy Policy ครอบคลุมทุกหน่วยงาน
- 2) ใช้ระบบ SSO + MFA ในการเข้าสู่ระบบสารสนเทศของมหาวิทยาลัย
- 3) จัดเวิร์กช็อปอบรม PDPA สำหรับเจ้าหน้าที่ที่เกี่ยวข้องกับข้อมูล เช่น ทะเบียน, พัสดุ, กิจการนักศึกษา
- 4) จัดทำ Incident Response Plan และแบบฟอร์มรายงานเหตุการณ์ตามข้อกำหนดของ NCSC

ตารางที่ 12 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

5.5.7 องค์ประกอบที่ 7: Ecosystem & Partnership

การพัฒนา มหาวิทยาลัยดิจิทัล ไม่สามารถเกิดขึ้นได้ด้วยการดำเนินงานภายในเพียงลำพัง การสร้างเครือข่ายความร่วมมือและระบบนิเวศ (Digital Ecosystem) ที่เชื่อมโยงกับภาครัฐ เอกชน ชุมชน และภาค การศึกษาร่วมกัน จึงกลายเป็นหัวใจสำคัญในการผลักดันให้เกิดนวัตกรรมดิจิทัลที่แท้จริง

Ecosystem & Partnership คือองค์ประกอบที่สะท้อนบทบาทของมหาวิทยาลัยในฐานะ แพลตฟอร์มของการพัฒนา ซึ่งต้องมีทั้งพันธมิตรทางเทคโนโลยี ผู้สนับสนุนทุนวิจัย ภาครัฐ และผู้มีส่วนได้ ส่วนเสียที่ร่วมกันสร้างประโยชน์จากระบบดิจิทัลร่วมกัน

▪ เป้าหมายหลัก

- 1) สร้างความร่วมมือระหว่างมหาวิทยาลัยกับพันธมิตรหลากหลายภาคส่วน
- 2) ส่งเสริมการใช้ทรัพยากรร่วมกันผ่านระบบดิจิทัล (Co-sharing)
- 3) เปิดพื้นที่ให้องค์กรเอกชนเข้ามามีส่วนร่วมในการพัฒนานวัตกรรม
- 4) สนับสนุนการเรียนรู้ การทำวิจัย และการพัฒนาทักษะดิจิทัลร่วมกัน

▪ แนวทางการดำเนินงาน

- 1) จัดทำ MOU / MOA กับภาคีภายนอก เช่น บริษัทเทคโนโลยี, หน่วยงานรัฐ, Startup, ภาคอุตสาหกรรม เพื่อร่วมวิจัย พัฒนาแพลตฟอร์ม หรือให้ทุนสนับสนุน
- 2) พัฒนา Open Innovation Platform ให้บุคลากร นักศึกษา และภาคีภายนอกสามารถร่วมกันแก้ปัญหา และทดสอบแนวคิดดิจิทัลใหม่ ๆ
- 3) เปิดให้ใช้ API / Open Data ภายใต้เงื่อนไขที่เหมาะสม เพื่อให้องค์กรภายนอกสามารถเชื่อมต่อบริการ หรือสร้างแอปพลิเคชันที่ใช้ประโยชน์จากข้อมูลภายในมหาวิทยาลัย
- 4) ตั้งหน่วยงานส่งเสริมนวัตกรรมร่วม (Innovation Hub) ทำหน้าที่กลางในการเชื่อมโยงมหาวิทยาลัยกับภาคีพันธมิตร ทั้งในระดับท้องถิ่นและระดับชาติ
- 5) ส่งเสริม Co-learning และ Co-research โดยเชิญผู้เชี่ยวชาญภายนอกมาร่วมสอน เสวนา หรือเป็นพี่เลี้ยงโครงการให้นักศึกษาและบุคลากร

▪ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) ทำความร่วมมือกับบริษัท IT ในการฝึกอบรม AI / Cloud Computing ให้บุคลากร
- 2) ร่วมมือกับองค์กรปกครองส่วนท้องถิ่น พัฒนาระบบจัดการข้อมูลชุมชน
- 3) สร้างโครงการ VRU Startup Sandbox เปิดให้นักศึกษาและชุมชนทดสอบแพลตฟอร์มดิจิทัล
- 4) ใช้ระบบ e-Internship ที่เชื่อมโยงกับบริษัทและภาคีเพื่อจัดการฝึกงานแบบออนไลน์

ตารางที่ 13 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

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

5.5.8 องค์ประกอบที่ 8: Monitoring, Evaluation & Improvement

ในระบบการบริหารยุคใหม่ การพัฒนาเชิงกลยุทธ์จะไม่มีวันสมบูรณ์หากขาดกระบวนการ ติดตาม ประเมินผล และปรับปรุง อย่างต่อเนื่อง เพราะเทคโนโลยีและความคาดหวังของผู้ใช้งานสามารถเปลี่ยนแปลงได้ตลอดเวลา

Monitoring, Evaluation & Improvement จึงเป็นองค์ประกอบสุดท้ายของ VRU-DUF ซึ่งทำหน้าที่เป็น กลไกควบคุมคุณภาพ และ ระบบป้อนกลับ เพื่อให้มหาวิทยาลัยสามารถตรวจสอบความก้าวหน้า ประเมินผลลัพธ์ และปรับเปลี่ยนแนวทางได้อย่างเหมาะสมตามบริบทจริง

■ เป้าหมายหลัก

- 1) มีระบบติดตามผลการดำเนินงานด้านดิจิทัลอย่างเป็นระบบและต่อเนื่อง
- 2) สามารถประเมินความก้าวหน้าและผลกระทบของแผนดิจิทัลได้ทั้งในระดับโครงการและระดับองค์กร
- 3) มีระบบปรับปรุงแผนงาน/กลยุทธ์ตามบริบทและสถานการณ์ที่เปลี่ยนแปลง
- 4) สร้างวัฒนธรรมองค์กรที่ยึดหลัก เรียนรู้และพัฒนาอย่างต่อเนื่อง

■ แนวทางการดำเนินงาน

- 1) จัดทำ Digital KPI Dashboard สำหรับแต่ละหน่วยงาน เช่น ร้อยละของบริการออนไลน์, ปริมาณการใช้งานแพลตฟอร์ม, ระยะเวลาการให้บริการ
- 2) จัดประชุม V-DUF Progress Review รายเดือนหรือรายไตรมาส เพื่อรายงานผลความคืบหน้า อุปสรรค และข้อเสนอแนะแก่คณะกรรมการกลาง
- 3) ทำ Self-Assessment โดยใช้ Digital Maturity Model เช่น แบบประเมินของ DGA, อว., หรือเครื่องมือที่พัฒนาเอง เพื่อวัดระดับความพร้อมทางดิจิทัลของแต่ละหน่วยงาน
- 4) ดำเนินการ Audit หรือ External Evaluation เพื่อให้เกิดมุมมองจากภายนอกและความน่าเชื่อถือของผลการประเมิน
- 5) วางระบบ Feedback Loop กับผู้ใช้งาน เช่น นักศึกษา บุคลากร อาจารย์ ผ่านแบบสอบถาม การสัมภาษณ์ หรือ Social Listening
- 6) อัปเดตแผนดิจิทัลเป็นประจำ (Rolling Plan) เพื่อให้แผนแม่บทสามารถปรับได้ตามบริบทและไม่ถูกทิ้งไว้เป็นเพียงเอกสารเชิงทฤษฎี

■ ตัวอย่างการประยุกต์ใช้ในมหาวิทยาลัย

- 1) พัฒนา VRU Digital Dashboard สำหรับติดตามตัวชี้วัดในแต่ละองค์ประกอบของ V-DUF
- 2) จัดประชุม VRU Digital Forum ทุกไตรมาส ให้แต่ละหน่วยงานรายงานผลงานดิจิทัลของตนเอง
- 3) ใช้แบบประเมินความพึงพอใจออนไลน์หลังการใช้บริการ เช่น e-Document, e-Service, LMS
- 4) แต่งตั้งทีมประเมินผลอิสระ เพื่อทบทวนความคุ้มค่าของโครงการและผลกระทบต่อผู้ใช้งาน

ตารางที่ 14 แสดงการเชื่อมโยงกับกรอบการทำงานภายนอก

กรอบการทำงาน	องค์ประกอบที่เกี่ยวข้อง
DGA Digital Government	Performance Monitoring, Maturity Assessment
มหาวิทยาลัย 4.0 (อว.)	Evaluation-Based Management
NIST CSF 2.0	Govern / Respond / Recover (Monitoring & Reporting)

6. แผนขับเคลื่อนมหาวิทยาลัยดิจิทัล (Digital University Plan)

เมื่อมหาวิทยาลัยฯ ได้วางกรอบทิศทางและกรอบแนวคิดการพัฒนาสู่มหาวิทยาลัยดิจิทัลผ่าน VRU Digital University Framework (V-DUF) ซึ่งประกอบด้วย 8 องค์ประกอบหลัก (DGL, DISC, DPS, PDC, DGI, CDP, EP และ MEI) แล้วนั้น สิ่งสำคัญลำดับถัดไปคือการแปลงแนวคิดไปสู่การปฏิบัติ อย่างเป็นรูปธรรม

แผนขับเคลื่อนฉบับนี้ถูกออกแบบให้สามารถ ดำเนินการในระยะเวลา 6 เดือน โดยมีจุดเน้นที่การวางรากฐานที่มั่นคง ครอบคลุมทุกมิติของระบบงาน และสร้างกลไกติดตามผลที่ชัดเจน เพื่อรองรับการขยายผลในระยะยาว

แผนนี้แบ่งการดำเนินงานออกเป็นรายเดือน และจัดวางกิจกรรมให้สอดคล้องกับองค์ประกอบของกรอบการทำงานV-DUF โดยใช้ชื่อย่อของแต่ละด้านเป็นแกนหลักในการวางโครงสร้างกิจกรรม ดังนี้

ตารางที่ 15 แสดง แผนการดำเนินงานของแต่ละอนุกรรมการ

	DGL (Governance & Leadership)	DISC (Infrastructure & Smart Campus)	DPS (Platform & Services)	PDC (People & Digital Culture)	DGI (Data Governance & Intelligence)	CDP (Cybersecurity & Data Privacy)	EP (Ecosystem & Partnership)	MEI (Monitoring & Evaluation)
เดือนที่ 1	ตั้งคณะกรรมการและทีม War Room	สำรวจโครงสร้างพื้นฐานเดิม	วิเคราะห์ระบบงานที่จำเป็น	สำรวจทักษะบุคลากร	กำหนด Data Owner & Data Set	กำหนดนโยบาย PDPA / Cybersecurity	วิเคราะห์ภาคีความร่วมมือเดิม	กำหนด KPI และแบบฟอร์มติดตาม
เดือนที่ 2	แต่งตั้ง CIO / CDO และจัดทำนโยบายดิจิทัล	วางแผนปรับปรุง Network/Wi-Fi	ออกแบบ Web Portal และ SSO	จัดอบรม Digital Literacy รอบแรก	ออกแบบ Data Lake / Dashboard	แต่งตั้ง DPO / CSIRT	เริ่มจัดทำ MOU / ประสานภาคี	ออกแบบ Dashboard ติดตามผล
เดือนที่ 3	จัดประชุมคณะกรรมการครั้งที่ 1	เริ่มติดตั้งอุปกรณ์พื้นฐาน (NAS, Switch)	พัฒนาระบบ e-Document / LMS	แต่งตั้ง Digital Ambassador	จัดทำ Metadata และโครงสร้างข้อมูล	วางมาตรการด้าน MFA และ Backup	จัดกิจกรรม Hackathon / ร่วมวิจัย	เริ่มเก็บ Feedback การใช้ระบบ
เดือนที่ 4	ประกาศนโยบาย Digital Transformation	ใช้งานระบบ SSO / e-Service เบื้องต้น	เปิดใช้ Portal ทดลอง	อบรม Advance Tools (AI, BI)	เปิดใช้ Dashboard นักศึกษา/บริหาร	จำลองเหตุการณ์ Cyber Incident	เปิดพื้นที่ทดสอบนวัตกรรม	ติดตามผลและปรับปรุง KPI
เดือนที่ 5	ตรวจสอบความคืบหน้าแผนภาพรวม	ขยายระบบ Smart Facility (IoT)	เชื่อมระบบอื่นเข้าสู่แพลตฟอร์มกลาง	อบรมเชิงลึกและ Coaching หน่วยงาน	เชื่อมข้อมูลฐานอื่น (HR, Finance)	ประเมิน PDPA Compliance เบื้องต้น	ลงนามความร่วมมือระดับจังหวัด/ชาติ	สรุปผลเบื้องต้นรายองค์ประกอบ
เดือนที่ 6	จัดประชุมใหญ่สรุปความก้าวหน้า	ประกาศใช้งานระบบดิจิทัลเต็มรูปแบบ	ประเมินความพึงพอใจการใช้บริการ	จัดนิทรรศการ/ประกวดนวัตกรรมดิจิทัล	สรุปผลการใช้ข้อมูลในองค์กร	ส่งรายงานประเมินผลความมั่นคง	ประเมินพันธมิตรและความยั่งยืน	ทบทวนและปรับแผนปีถัดไป

แผนการดำเนินการ (Action Plan)

■ เดือนที่ 1: วางรากฐานการขับเคลื่อน

DGL: แต่งตั้งคณะกรรมการขับเคลื่อน V-DUF และทีม War Room ดิจิทัล พร้อมจัดประชุมชี้แจงนโยบายเบื้องต้น

DISC: สำรวจและประเมินสถานะโครงสร้างพื้นฐานเดิม (Network, Server, Wi-Fi)

DPS: วิเคราะห์ระบบงานที่ควรพัฒนาในรูปแบบ Platform เช่น e-Document, SSO

PDC: สำรวจทักษะดิจิทัลของบุคลากร และความพร้อมในการเปลี่ยนผ่าน

DGI: กำหนด Data Owner และจัดทำบัญชีชุดข้อมูลหลัก (Master Data Set)

CDP: ร่างนโยบาย PDPA และ Cybersecurity เบื้องต้น พร้อมวางแผนทางแต่งตั้ง DPO / CSIRT

EP: ทบทวนพันธมิตรที่มีอยู่ และตั้งเป้าหมายความร่วมมือใหม่

MEI: กำหนดตัวชี้วัดระดับองค์กร และออกแบบฟอร์มติดตามผลรายเดือน

■ เดือนที่ 2: วางระบบเชิงโครงสร้างและแนวนโยบาย

DGL: แต่งตั้ง CIO / CDO อย่างเป็นทางการ พร้อมประกาศแนวนโยบายดิจิทัลของมหาวิทยาลัย

DISC: จัดทำแผนปรับปรุงระบบ Network / Wi-Fi / Server / Cloud

DPS: ออกแบบ Web Portal กลาง และระบบ Single Sign-On

PDC: จัดอบรม Digital Literacy รอบแรกสำหรับบุคลากรทุกสาย

DGI: เริ่มออกแบบ Data Lake และ Dashboard สำหรับผู้บริหาร

CDP: แต่งตั้ง DPO / จัดทีม CSIRT / วางระบบการแจ้งเหตุผิดปกติ

EP: ดำเนินการร่าง MOU กับหน่วยงานภายนอก (ภาครัฐ-เอกชน)

MEI: ออกแบบ Dashboard ติดตามผลเบื้องต้น และระบบเก็บ Feedback

■ เดือนที่ 3: เริ่มต้นพัฒนาและทดสอบระบบ

DGL: จัดประชุมคณะกรรมการขับเคลื่อนครั้งแรกอย่างเป็นทางการ

DISC: เริ่มติดตั้งอุปกรณ์พื้นฐาน เช่น NAS, Switch, AP Wi-Fi

DPS: เริ่มพัฒนาระบบ e-Document และ LMS เวอร์ชันต้นแบบ

PDC: แต่งตั้ง Digital Ambassador ประจำคณะ/หน่วยงาน

DGI: จัดทำ Metadata / Data Dictionary กลางขององค์กร

CDP: วางมาตรการ MFA, Backup, และ DR เบื้องต้น

EP: จัดกิจกรรม Hackathon / Co-Design กับภาคีเครือข่าย

MEI: เริ่มเก็บข้อมูลการใช้งานระบบ และผลตอบรับเบื้องต้น

■ เดือนที่ 4: เปิดใช้ระบบต้นแบบและสร้างแรงกระเพื่อม

DGL: ประกาศวิสัยทัศน์ Digital Transformation อย่างเป็นทางการ

DISC: เปิดใช้งานระบบ SSO และ e-Service เบื้องต้น

DPS: เปิดให้ทดลองใช้ Web Portal และระบบงานบางส่วน

PDC: จัดอบรมทักษะระดับสูง เช่น AI, BI, Microsoft Power Platform

DGI: เปิดใช้งาน Dashboard นักศึกษา / ผู้บริหารบางรายการ

CDP: จัดซ้อมแผนเผชิญเหตุด้าน Cybersecurity

EP: เปิดพื้นที่นวัตกรรม Sandbox ให้นักศึกษา/ภาคีทดสอบโครงการ

MEI: ติดตามผลการดำเนินงาน และจัดประชุมสะท้อนผล (Reflection)

▪ เดือนที่ 5: ขยายผลสู่ระบบเต็มรูปแบบ

DGL: ตรวจสอบความก้าวหน้าและจัดประชุมติดตามเชิงลึก
 DISC: ขยายระบบ Smart Facility เช่น IoT, ระบบเข้า-ออกอาคาร
 DPS: เชื่อมต่อระบบงานอื่นเข้าสู่ Web Portal และ Data Lake
 PDC: จัดอบรมเชิงลึกและให้คำปรึกษารายหน่วยงาน
 DGI: เชื่อมข้อมูลฐานอื่น เช่น การเงิน, HR, วิจัย
 CDP: ประเมินความสอดคล้องกับ PDPA และ NIST CSF 2.0
 EP: ดำเนินความร่วมมือกับหน่วยงานระดับจังหวัด / อุตสาหกรรม
 MEI: รวบรวมข้อมูลผลลัพธ์รายองค์ประกอบ เตรียมสรุปรายงานใหญ่

▪ เดือนที่ 6: สรุปผลและเตรียมขยายผลต่อยอด

DGL: จัดประชุมสรุปความก้าวหน้าของคณะกรรมการ V-DUF
 DISC: เปิดใช้งานระบบโครงสร้างพื้นฐานเต็มรูปแบบ
 DPS: ประกาศเปิดใช้งานระบบดิจิทัลอย่างเป็นทางการ
 PDC: จัดนิทรรศการ/ประกวดนวัตกรรมของบุคลากร/นักศึกษา
 DGI: สรุปผลการใช้งาน Dashboard / ข้อมูลเชิงวิเคราะห์
 CDP: ส่งรายงานผลประเมินความปลอดภัยต่อผู้บริหาร
 EP: ประเมินความสัมพันธ์กับพันธมิตร และแผนความยั่งยืน
 MEI: สรุปบทเรียน ปรับแผนต่อเนื่อง และจัดทำแผนปีถัดไป

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 องค์ประกอบตามกรอบ V-DUF เพื่อให้การบริหารสามารถกระจายอำนาจ กำหนดบทบาทอย่างชัดเจน และส่งเสริมการมีส่วนร่วมจากทุกหน่วยงานในมหาวิทยาลัย

7.1. คณะกรรมการอำนวยการมหาวิทยาลัยดิจิทัล (Digital University Executive Board)

บทบาท: กำหนดนโยบาย วิสัยทัศน์ เป้าหมายสูงสุด อนุมัติแผนแม่บท และกำกับทิศทางรวมขององค์กร
 องค์ประกอบแนะนำ:

- 1) อธิการบดี (ประธาน)
- 2) รองอธิการบดีทุกฝ่าย (รองประธาน)
- 3) ผู้อำนวยการสำนักงานอธิการบดี
- 4) ผู้อำนวยการสำนักยุทธศาสตร์
- 5) ผู้อำนวยการศูนย์คอมพิวเตอร์
- 6) เลขานุการ: ผู้ช่วยอธิการบดีฝ่ายดิจิทัล / CIO

7.2 คณะกรรมการขับเคลื่อน V-DUF (Digital Transformation Steering Committee)

บทบาท: วางแผนระดับยุทธศาสตร์ ออกแบบโครงการ กำกับติดตามการดำเนินงานรายเดือน รวบรวมรายงานจาก
 อนุกรรมการทั้ง 8 ชุด

องค์ประกอบแนะนำ:

- 1) ผู้ช่วยอธิการบดีฝ่ายดิจิทัล (ประธาน)
- 2) CIO / CDO / ผู้อำนวยการศูนย์คอมพิวเตอร์ (กรรมการ/เลขานุการ)
- 3) หัวหน้าสำนัก/สาขาวิชาหลัก (เช่น ทะเบียน, บุคลากร, การเงิน)
- 4) ตัวแทนฝ่ายวิชาการ / ฝ่ายพัฒนานักศึกษา
- 5) นักวิชาการอาวุโสด้านเทคโนโลยี / วางแผน / นวัตกรรม

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) รองอธิการบดี / ผู้ช่วยอธิการบดี
- 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) ผอ. ศูนย์คอมพิวเตอร์
- 2) วิศวกรเครือข่าย / นักคอมฯ ด้านโครงสร้างพื้นฐาน
- 3) หัวหน้าหน่วยอาคาร / สาธารณูปโภค
- 4) เจ้าหน้าที่ Smart Campus

▪ 3) อนุกรรมการ DPS (Platform & Services)

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

ประกอบด้วย:

- 1) หัวหน้าหน่วยงานทะเบียน, การเงิน, บุคลากร
- 2) นักพัฒนาระบบ / Full Stack / Laravel / Dev
- 3) ตัวแทนสายวิชาการผู้ใช้งาน
- 4) นักศึกษาตัวแทน / user tester

▪ 4) อนุกรรมการ PDC (People & Digital Culture)

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

ประกอบด้วย:

- 1) ผอ. สำนักทรัพยากรบุคคล
- 2) หัวหน้าฝ่ายพัฒนาอาจารย์ / ฝึกอบรม
- 3) ตัวแทนคณะ / สาขาวิชา

4) นักวิชาการพัฒนาองค์กร

▪ 5) อนุกรรมการ DGI (Data Governance & Intelligence)

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

ประกอบด้วย:

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

▪ 6) อนุกรรมการ CDP (Cybersecurity & Data Privacy)

หน้าที่: ดำเนินการด้าน NIST CSF, PDPA, ความมั่นคงปลอดภัยไซเบอร์

ประกอบด้วย:

- 1) DPO (เจ้าหน้าที่ PDPA)
- 2) หัวหน้าทีม CSIRT / Cyber Response
- 3) ตัวแทนฝ่ายกฎหมาย / นิติกร
- 4) นักคอมพิวเตอร์ ระบบและความปลอดภัย

▪ 7) อนุกรรมการ EP (Ecosystem & Partnership)

หน้าที่: ประสานความร่วมมือ MOU, Sandbox, Open Innovation

ประกอบด้วย:

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

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

หน้าที่: ติดตามผล, ประเมิน, จัดทำ Dashboard, สรุปบทเรียน

ประกอบด้วย:

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

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 รายหน่วยงาน
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. PDC (People & Digital Culture)	- แผนพัฒนาทักษะบุคลากร (Digital Literacy / AI / BI) - ตารางอบรม, เอกสารประกอบการฝึกอบรม - รายชื่อ Digital Ambassador - แผนสร้างวัฒนธรรมดิจิทัลองค์กร
5. DGI (Data Governance & Intelligence)	- รายชื่อ Data Owner / Steward - Metadata / Data Dictionary (ฉบับแรก) - แผนพัฒนา Data Lake / Dashboard - ตัวอย่าง Dashboard สำหรับผู้บริหาร
6. CDP (Cybersecurity & Data Privacy)	- แต่งตั้ง DPO, ทีม CSIRT พร้อม TOR - นโยบาย PDPA และนโยบายความมั่นคงปลอดภัยไซเบอร์ - รายงานความเสี่ยง / แผนตอบสนองเหตุการณ์ (Incident Plan) - ผลการซ้อมระบบ / การอบรมด้านความปลอดภัย
7. EP (Ecosystem & Partnership)	- รายชื่อพันธมิตรหลักภายใน/ภายนอก - MOU ที่ลงนาม / ร่าง MOU - แผนพัฒนา Sandbox / Innovation Space - กิจกรรมความร่วมมือ / Hackathon / Co-research
8. MEI (Monitoring, Evaluation & Improvement)	- แผนการติดตามและประเมินผล V-DUF - Dashboard ติดตามผลรายองค์ประกอบ - รายงานความก้าวหน้า (รายเดือน/ไตรมาส) - สรุปบทเรียน / แผนปรับปรุงต่อเนื่อง (Rolling Plan)

ปรับปรุงล่าสุด วันที่ 18 พฤษภาคม 2568

จัดทำโดย

ผู้ช่วยศาสตราจารย์ ดร.เศรษฐพงศ์ วงษ์อินทร์

ตารางติดตามผลอนุกรรมการ V-DUF

อนุกรรมการ	เอกสารที่ต้องส่ง	รหัสเอกสารหลัก
DGL (Governance & Leadership)	นโยบายการขับเคลื่อน แผนแม่บทมหาวิทยาลัยดิจิทัล คำสั่งแต่งตั้งกรรมการ ตัวชี้วัดดิจิทัล	DGL-Po (Policy) DGL-MP (Master Plan) DGL-Or (Order) DGL-KPI
DISC (Infrastructure & Smart Campus)	แผนโครงสร้างพื้นฐาน IT รายงานสำรวจระบบเดิม ผังโครงข่ายและอุปกรณ์	DISC-Plan DISC-Survey DISC-NetMap
DPS (Platform & Services)	รายชื่อระบบที่พัฒนา แผนเชื่อมโยงระบบ คู่มือใช้งานระบบ	DPS-SysList DPS-Intg (Integration Plan) DPS-Manual
PDC (People & Digital Culture)	แผนอบรมบุคลากร รายชื่อ Digital Ambassador รายงานผลการอบรม	PDC-TrainPlan PDC-AmbList PDC-TrainRpt
DGI (Data Governance & Intelligence)	Metadata และ Dictionary แผนพัฒนา Dashboard ตัวอย่าง Dashboard	DGI-Meta DGI-DashPlan DGI-DashDemo
CDP (Cybersecurity & Data Privacy)	นโยบาย PDPA / Cybersecurity แผนตอบสนองเหตุการณ์ รายงานซ้อมระบบ	CDP-Pol CDP-IncidentPlan CDP-DrillRpt
EP (Ecosystem & Partnership)	รายชื่อพันธมิตร ร่าง/ฉบับจริงของ MOU รายงานกิจกรรมร่วมมือ	EP-PartnerList EP-MOU EP-ActRpt
MEI (Monitoring & Evaluation)	แผนติดตามผล Dashboard ติดตาม สรุปผลการดำเนินงาน	MEI (Monitoring & Evaluation)