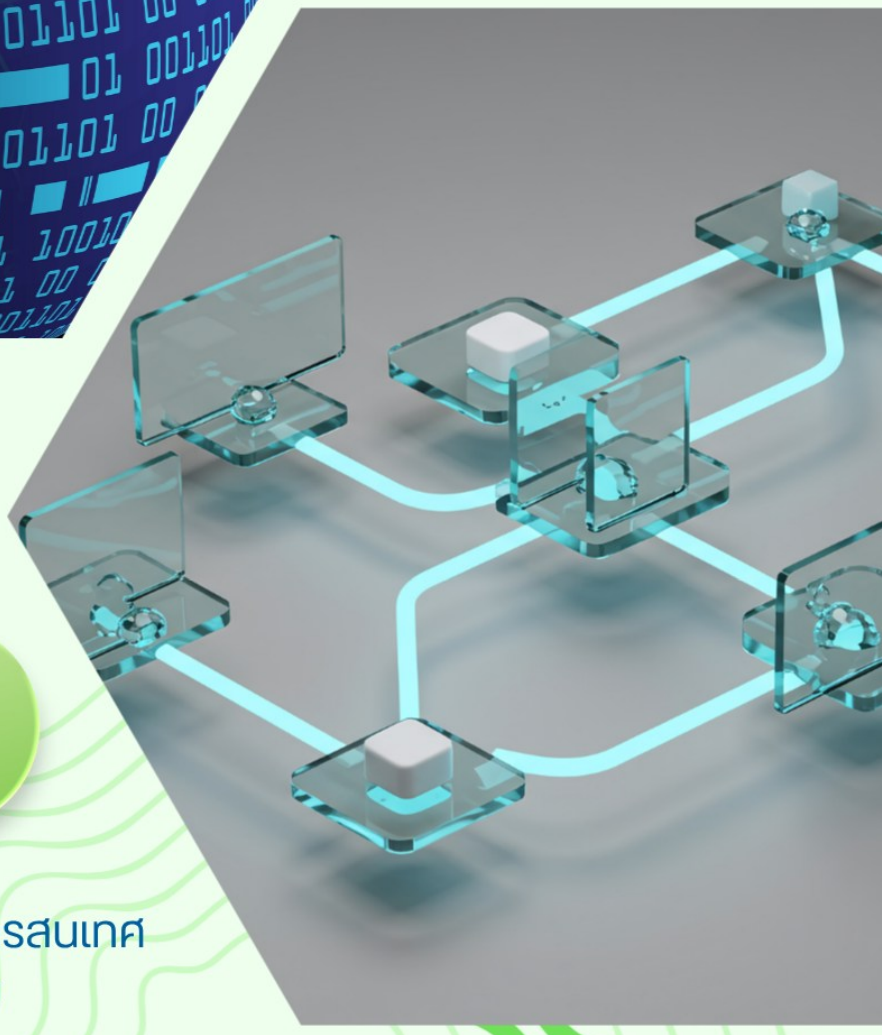
รายงานผลการวิเคราะห์ความเสี่ยง
คลังสารสนเทศดิจิทัลพิบูลสงคราม



ปี พ.ศ. 2568

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏพิบูลสงคราม

คำนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อศึกษาและวิเคราะห์สถานการณ์ของคลังสารสนเทศดิจิทัลมหาวิทยาลัยราชภัฏพิบูลสงคราม โดยมุ่งเน้นการใช้เครื่องมือ SWOT Analysis และ TOWS Matrix เป็นแนวทางในการประเมินสภาพแวดล้อมทั้งภายในและภายนอกของระบบคลังสารสนเทศ เพื่อระบุจุดแข็ง จุดอ่อน โอกาส และอุปสรรคที่ส่งผลต่อการบริหารจัดการและการพัฒนาโครงสร้างพื้นฐานสารสนเทศของมหาวิทยาลัย ทั้งนี้เพื่อให้สามารถกำหนดกลยุทธ์ในการพัฒนาและจัดการความเสี่ยงได้อย่างเหมาะสม สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีดิจิทัลในปัจจุบัน รายงานฉบับนี้จึงมีจุดมุ่งหมายเพื่อเป็นแนวทางในการยกระดับคลังสารสนเทศดิจิทัลให้มีความมั่นคงปลอดภัย ทันสมัย และตอบสนองต่อเป้าหมายของมหาวิทยาลัยในการก้าวสู่การเป็น “มหาวิทยาลัยดิจิทัล” อย่างมีประสิทธิภาพและยั่งยืน ผู้จัดทำหวังเป็นอย่างยิ่งว่ารายงานฉบับนี้จะเป็นประโยชน์ต่อผู้บริหาร บุคลากรทางเทคโนโลยีสารสนเทศ ตลอดจนผู้ที่เกี่ยวข้องในการพัฒนาคลังสารสนเทศดิจิทัลของมหาวิทยาลัยต่อไป

คณะทำงานคลังสารสนเทศดิจิทัลพิบูลสงคราม

สารบัญ

บทนำ

คลังสารสนเทศดิจิทัลของมหาวิทยาลัยราชภัฏพิบูลสงครามเป็นแหล่งรวบรวม จัดเก็บ และให้บริการข้อมูลทางวิชาการในรูปแบบอิเล็กทรอนิกส์ เพื่อสนับสนุนภารกิจหลักด้านการเรียนการสอน การวิจัย และการบริการวิชาการแก่สังคม โดยมีบทบาทสำคัญในการเป็นศูนย์กลางข้อมูลที่ช่วยอำนวยความสะดวกในการเข้าถึงสารสนเทศได้อย่างรวดเร็วและทั่วถึง ทั้งนี้ ในยุคที่เทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างต่อเนื่องและรวดเร็ว การบริหารจัดการคลังสารสนเทศดิจิทัลจึงจำเป็นต้องมีกลยุทธ์ที่รอบคอบและยืดหยุ่น เพื่อให้ระบบสามารถรองรับความต้องการของผู้ใช้ได้อย่างมีประสิทธิภาพ ปลอดภัย และตอบโจทย์การพัฒนามหาวิทยาลัยสู่ความเป็นมหาวิทยาลัยดิจิทัลอย่างสมบูรณ์

หลักการและเหตุผล

ในปัจจุบัน การเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศส่งผลให้รูปแบบการจัดเก็บและให้บริการข้อมูลเปลี่ยนแปลงจากระบบเอกสารแบบดั้งเดิมไปสู่ระบบดิจิทัล ซึ่งแม้จะเพิ่มความสะดวกในการเข้าถึงข้อมูล แต่ก็มีความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลและการบริหารจัดการระบบที่ซับซ้อนมากขึ้น ดังนั้น การวิเคราะห์สถานการณ์ของคลังสารสนเทศดิจิทัลด้วยเครื่องมือ SWOT (Strengths, Weaknesses, Opportunities, Threats) และ TOWS Matrix จึงเป็นแนวทางสำคัญในการประเมินสภาพแวดล้อมทั้งภายในและภายนอก เพื่อระบุจุดแข็ง จุดอ่อน โอกาส และอุปสรรคในการดำเนินงาน อันจะนำไปสู่การกำหนดกลยุทธ์ในการบริหารจัดการความเสี่ยงและการพัฒนาระบบให้มีความมั่นคง ปลอดภัย ทันสมัย และสอดคล้องกับวิสัยทัศน์ของมหาวิทยาลัยราชภัฏพิบูลสงครามในการมุ่งสู่การเป็น “มหาวิทยาลัยดิจิทัล” ที่มีความยั่งยืนในอนาคต

วัตถุประสงค์

1. เพื่อวิเคราะห์สภาพแวดล้อมภายในและภายนอกของคลังสารสนเทศดิจิทัล โดยใช้เครื่องมือ SWOT และ TOWS Matrix
2. เพื่อระบุและประเมินปัจจัยเสี่ยงที่อาจส่งผลต่อความมั่นคงและประสิทธิภาพของระบบสารสนเทศ เพื่อกำหนดแนวทางและกลยุทธ์ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีและข้อมูลสารสนเทศอย่างเหมาะสม
3. เพื่อพัฒนาโครงการและกิจกรรมรองรับการจัดการความเสี่ยงให้สอดคล้องกับนโยบาย “มหาวิทยาลัยดิจิทัล”
4. เพื่อยกระดับคลังสารสนเทศดิจิทัลให้เป็นศูนย์กลางความรู้ที่ปลอดภัย ทันสมัย และยั่งยืนของมหาวิทยาลัยราชภัฏพิบูลสงคราม

การวิเคราะห์สภาพแวดล้อม (SWOT Analysis)

จุดแข็ง (Strengths)

1. มีโครงสร้างพื้นฐานด้านเทคโนโลยีที่มั่นคงพอสมควร เช่น ระบบเครือข่ายภายในมหาวิทยาลัย (LAN/Wi-Fi) และระบบ Server กลางที่ดูแลโดยผู้เชี่ยวชาญ

2. มีบุคลากรที่มีความรู้ด้านเทคโนโลยีสารสนเทศและการจัดการฐานข้อมูล เจ้าหน้าที่สามารถดูแลระบบคลังสารสนเทศและบริการได้อย่างมีประสิทธิภาพ

3. มีนโยบายสนับสนุนจากผู้บริหารมหาวิทยาลัย มหาวิทยาลัยมีเป้าหมายมุ่งสู่การเป็น “มหาวิทยาลัยดิจิทัล” (Digital University)

4. ระบบคลังสารสนเทศมีความหลากหลายของข้อมูล เช่น วิทยานิพนธ์ งานวิจัย บทความ เอกสารอ้างอิง ฯลฯ ทำให้เป็นศูนย์กลางองค์ความรู้ของมหาวิทยาลัย

5. มีการสำรองข้อมูลเป็นระยะ (Backup System) ช่วยลดความเสี่ยงจากการสูญหายของข้อมูลสำคัญ

6. มีระบบกำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

จุดอ่อน (Weaknesses)

1. ระบบความปลอดภัยไซเบอร์ (Cybersecurity) ยังไม่สมบูรณ์ เช่น ขาดระบบตรวจจับการบุกรุก (IDS/IPS) หรือระบบบันทึก Log ที่ครอบคลุม

2. ขาดบุคลากรเฉพาะทางด้านความมั่นคงปลอดภัยข้อมูล เจ้าหน้าที่ IT ต้องรับผิดชอบหลายด้าน ทำให้การเฝ้าระวังความเสี่ยงไม่ต่อเนื่อง

3. การสำรองข้อมูลอาจยังไม่ครอบคลุมทุกระบบหรือยังอยู่ในรูปแบบ Manual ทำให้มีช่องโหว่เมื่อเกิดเหตุฉุกเฉิน

4. งบประมาณด้านเทคโนโลยีและความปลอดภัยข้อมูลมีจำกัด ส่งผลต่อการจัดซื้อระบบรักษาความปลอดภัยระดับสูง

5. การสร้างความตระหนักรู้ด้านความปลอดภัยของบุคลากรและผู้ใช้ยังไม่เพียงพอ เช่น การตั้งรหัสผ่านไม่ปลอดภัย หรือการเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต

6. ไม่มีแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เมื่อระบบล่มหรือถูกโจมตี การฟื้นฟูอาจล่าช้า

โอกาส (Opportunities)

1. แนวโน้มของมหาวิทยาลัยทั่วประเทศมุ่งสู่ Digital Transformation ทำให้สามารถของบประมาณสนับสนุนโครงการพัฒนาคลังสารสนเทศได้

2. มีโอกาสร่วมมือกับหน่วยงานภายนอก เช่น ThaiLIS ในการพัฒนาและเชื่อมโยงฐานข้อมูลระดับชาติ

3. เทคโนโลยี Cloud และปัญญาประดิษฐ์ AI เข้ามาช่วยเสริมระบบคลังข้อมูลให้มีประสิทธิภาพสูงขึ้น เช่น Cloud Backup, AI Metadata Tagging, ระบบสืบค้นอัจฉริยะ

4. มีโอกาสจัดอบรมและพัฒนาบุคลากรผ่านหลักสูตรออนไลน์ (e-Learning) เพิ่มทักษะด้านความมั่นคงปลอดภัยข้อมูลและการจัดการสารสนเทศ

5. แนวโน้มผู้ใช้บริการเข้าถึงทรัพยากรดิจิทัลมากขึ้น ทำให้ระบบมีความสำคัญและได้รับการพัฒนาอย่างต่อเนื่องจากความต้องการของผู้ใช้

อุปสรรค (Threats)

1. ภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเพิ่มขึ้นอย่างต่อเนื่อง เช่น Ransomware, Phishing, Malware, การโจมตีผ่านระบบเครือข่าย

2. ความเสี่ยงจากภัยธรรมชาติหรือเหตุฉุกเฉินทางกายภาพ เช่น ไฟไหม้ น้ำท่วม ไฟฟ้าดับ ทำให้ระบบไม่สามารถทำงานได้

3. การเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว ทำให้ระบบที่ใช้อยู่ล้าสมัยหากไม่มีการปรับปรุงต่อเนื่อง

4. การละเมิดข้อมูลส่วนบุคคล (PDPA Risk) หากไม่มีมาตรการคุ้มครองข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. ความเสี่ยงจากบุคคลภายใน (Insider Threat) เช่น การเข้าถึงข้อมูลโดยมิชอบ การคัดลอกข้อมูลออกนอกระบบโดยไม่อนุญาต

6. งบประมาณภาครัฐและนโยบายอาจเปลี่ยนแปลง ส่งผลต่อการต่อยอดและบำรุงรักษาระบบระยะยาว

การวิเคราะห์ TOWS Matrix จากผลการวิเคราะห์สภาพแวดล้อม (SWOT Analysis) สำหรับคลังสารสนเทศดิจิทัลของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม เพื่อให้เกิดแนวทางเชิงกลยุทธ์ และแนวปฏิบัติการจัดการความเสี่ยง มีดังนี้

ประเภทกลยุทธ์	การจับคู่ปัจจัย	แนวทางเชิงกลยุทธ์ / แนวปฏิบัติการจัดการความเสี่ยง
1. SO Strategy (ใช้จุดแข็งคว้าโอกาส)	S + O	กลยุทธ์เชิงรุก (Aggressive Strategy) 1. ใช้ระบบโครงสร้างพื้นฐานที่มั่นคง (S1) และบุคลากรที่เชี่ยวชาญ (S2) พัฒนาระบบคลังสารสนเทศดิจิทัลแบบ Cloud-Based เพื่อรองรับ Digital Transformation ของมหาวิทยาลัย (O1, O3) 2. ใช้การสนับสนุนจากผู้บริหาร (S3) ขับเคลื่อนโครงการ “Digital University Knowledge Hub” เพื่อเชื่อมโยงกับ ThaiLIS และฐานข้อมูลระดับชาติ (O2) 3. ใช้ความหลากหลายของข้อมูลในคลัง (S4) ร่วมกับเทคโนโลยี AI Metadata Tagging (O3) เพื่อเพิ่มคุณภาพและประสิทธิภาพในการสืบค้นข้อมูล 4. ใช้ระบบสำรองข้อมูลและการกำหนดสิทธิ์เข้าถึง (S5, S6) เพื่อเพิ่มความน่าเชื่อถือของระบบเมื่อมีการเปิดให้บริการแก่ผู้ใช้ที่เพิ่มขึ้น (O5)
2. WO Strategy (ใช้โอกาสเพื่อแก้จุดอ่อน)	W + O	กลยุทธ์เชิงพัฒนา (Improvement Strategy) 1. ใช้โอกาสจาก Digital Transformation (O1) เพื่อจัดสรรงบประมาณเสริมระบบความปลอดภัยไซเบอร์ (Cybersecurity Infrastructure) เช่น IDS/IPS, Firewall, SIEM (W1) 2. สร้างความร่วมมือกับ ThaiLIS หรือหน่วยงานภายนอก เพื่อให้บุคลากรได้รับการอบรมเฉพาะทางด้านความปลอดภัยข้อมูล (W2, O2, O4) 3. นำเทคโนโลยี Cloud Backup (O3) มาแทนระบบสำรองข้อมูลแบบ Manual (W3) 4. จัดทำหลักสูตร e-Learning ด้านความมั่นคง

		ปลอดภัยสารสนเทศ (Information Security Awareness) ให้บุคลากรและผู้ใช้บริการ (W5, O4). 5. ใช้แนวโน้มผู้ใช้บริการดิจิทัลที่เพิ่มขึ้น (O5) เป็นแรงผลักดันในการพัฒนาระบบบริการและการตอบสนองต่อผู้ใช้ (W4)
3. ST Strategy (ใช้จุดแข็งเพื่อลดอุปสรรค)	S + T	กลยุทธ์เชิงป้องกัน (Protective Strategy) 1. ใช้ระบบสำรองข้อมูล (S5) และระบบ Access Control (S6) เพื่อป้องกันภัยคุกคามไซเบอร์ เช่น Ransomware, Insider Threat (T1, T5) 2. ใช้บุคลากรที่มีความรู้ด้านเทคโนโลยี (S2) วางแผนและทดสอบ Disaster Recovery Plan (DRP) และ Business Continuity Plan (BCP) เพื่อรับมือภัยธรรมชาติ (T2) 3. ใช้นโยบาย Digital University (S3) เป็นกรอบในการพัฒนามาตรฐาน PDPA Compliance และการจัดเก็บข้อมูลส่วนบุคคล (T4) 4. ใช้ระบบโครงสร้างพื้นฐานที่มีเสถียรภาพ (S1) เพื่อรองรับการเปลี่ยนแปลงเทคโนโลยีอย่างต่อเนื่อง (T3)
4. WT Strategy (ลดจุดอ่อนและหลีกเลี่ยงอุปสรรค)	W + T	กลยุทธ์เชิงรับ (Defensive / Survival Strategy) 1. จัดทำ Risk Register และ ระบบตรวจสอบ Log อัตโนมัติ (Monitoring System) เพื่อเฝ้าระวังภัยไซเบอร์ในสภาพบุคลากรจำกัด (W1, W2, T1) 2. พัฒนาระบบสำรองข้อมูลอัตโนมัติและจัดเก็บนอกสถานที่ (Off-site Backup) เพื่อรองรับภัยธรรมชาติ (W3, T2) 3. จัดทำแผนงบประมาณระยะยาวเพื่อรองรับความเปลี่ยนแปลงนโยบายภาครัฐ (W4, T6) 4. จัดโครงการฝึกอบรมและสร้างความตระหนักด้านความปลอดภัยข้อมูล เพื่อป้องกันภัยจากบุคคลภายใน (W5, T5) 5. ใช้การกำหนดสิทธิ์เข้าถึง (S6) ร่วมกับนโยบาย PDPA เพื่อลดความเสี่ยงจากการละเมิดข้อมูล (T4)

หลังจากวิเคราะห์ SWOT และ TOWS แล้ว นำมาสู่การกำหนดโครงการและกิจกรรมรองรับแนวทางจัดการความเสี่ยง” เพื่อให้คลังสารสนเทศดิจิทัลของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงครามสามารถ พัฒนา ป้องกัน และตอบสนองต่อความเสี่ยงได้อย่างเป็นระบบ ดังนี้

1. SO Strategy (ใช้จุดแข็งเพื่อคว้าโอกาส)

แนวทาง : พัฒนาเชิงรุก เพื่อยกระดับคลังสารสนเทศสู่ระบบดิจิทัลเต็มรูปแบบ

โครงการ/กิจกรรม	วัตถุประสงค์	แนวทางการจัดการความเสี่ยง
1. โครงการพัฒนาคลังสารสนเทศดิจิทัลสู่ระบบ Cloud (Digital Knowledge Cloud Project)	เพื่อเพิ่มประสิทธิภาพในการจัดเก็บและให้บริการข้อมูลดิจิทัล	ลดความเสี่ยงจากระบบจัดเก็บข้อมูลแบบเดิมที่อาจสูญหาย และเพิ่มความต่อเนื่องในการให้บริการ
2. โครงการเชื่อมโยงฐานข้อมูลความรู้ระดับชาติ (ThaiLIS Integration Project)	เพื่อให้ข้อมูลวิชาการของมหาวิทยาลัยสามารถเข้าถึงได้ในระดับประเทศ	เพิ่มความน่าเชื่อถือและลดความเสี่ยงจากการขาดการเผยแพร่ข้อมูลสู่สาธารณะ
3. โครงการพัฒนาระบบสืบค้นอัจฉริยะด้วย AI (Smart Search & AI Tagging System)	เพื่อเพิ่มคุณภาพและความเร็วในการค้นคืนข้อมูล	ลดความเสี่ยงจากการค้นหาข้อมูลผิดพลาดและเพิ่มประสิทธิภาพผู้ใช้

2. WO Strategy (ใช้โอกาสเพื่อแก้จุดอ่อน)

แนวทาง : เสริมระบบ ความปลอดภัย และศักยภาพบุคลากร

โครงการ/กิจกรรม	วัตถุประสงค์	แนวทางการจัดการความเสี่ยง
1. โครงการพัฒนาระบบความปลอดภัยสารสนเทศ (Cybersecurity Enhancement Project)	เพื่อเพิ่มมาตรการป้องกันภัยไซเบอร์ เช่น IDS/IPS, Firewall, Monitoring	ลดความเสี่ยงจากการโจมตีทางไซเบอร์และข้อมูลรั่วไหล
2. โครงการอบรมบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Training)	เพื่อพัฒนาทักษะบุคลากรให้มีความรู้เฉพาะด้าน	ลดความเสี่ยงจากความผิดพลาดของบุคลากร
3. โครงการพัฒนาระบบสำรองข้อมูลอัตโนมัติ (Auto Backup & Recovery System)	เพื่อให้สามารถกู้คืนข้อมูลได้รวดเร็วในกรณีฉุกเฉิน	ลดความเสี่ยงจากการสูญหายของข้อมูล
4. โครงการสร้างความตระหนักรู้ด้านความปลอดภัยสารสนเทศ (Cyber Awareness Campaign)	เพื่อสร้างวัฒนธรรมความปลอดภัยในองค์กร	ลดความเสี่ยงจากพฤติกรรมผู้ใช้ เช่น การตั้งรหัสผ่านอ่อนแอ

3. ST Strategy (ใช้จุดแข็งเพื่อลดอุปสรรค)

แนวทาง : ใช้ศักยภาพภายในเพื่อรับมือภัยคุกคามและเหตุฉุกเฉิน

โครงการ/กิจกรรม	วัตถุประสงค์	แนวทางการจัดการความเสี่ยง
1. โครงการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity & Disaster Recovery Plan)	เพื่อเตรียมความพร้อมและฟื้นฟูระบบหลังภัยพิบัติ	ลดความเสี่ยงจากภัยธรรมชาติและเหตุขัดข้องทางเทคนิค
2. โครงการจัดทำมาตรฐาน PDPA และนโยบายการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance Policy)	เพื่อให้การจัดการข้อมูลเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ลดความเสี่ยงด้านกฎหมายและชื่อเสียงขององค์กร
3. โครงการทดสอบระบบความปลอดภัยและจำลองสถานการณ์ภัยคุกคาม (Penetration Test & Cyber Drill)	เพื่อทดสอบความพร้อมของระบบและทีมงาน	ลดความเสี่ยงจากการโจมตีจริง และตรวจพบช่องโหว่ก่อนเกิดเหตุ

4. WT Strategy (ลดจุดอ่อนและหลีกเลี่ยงอุปสรรค)

แนวทาง : เน้นป้องกันและรักษาความยั่งยืนระบบระยะยาว

โครงการ/กิจกรรม	วัตถุประสงค์	แนวทางการจัดการความเสี่ยง
1. โครงการจัดทำทะเบียนความเสี่ยง (Risk Register System)	เพื่อรวบรวม วิเคราะห์ และติดตามความเสี่ยงภายในระบบสารสนเทศ	ลดความเสี่ยงจากการขาดการควบคุมและติดตาม
2. โครงการติดตั้งระบบเฝ้าระวังและแจ้งเตือนภัยไซเบอร์อัตโนมัติ (Security Monitoring & Alert System)	เพื่อให้ตรวจจับเหตุผิดปกติได้แบบ Real-time	ลดระยะเวลาในการตอบสนองต่อภัยไซเบอร์
3. โครงการวางแผนงบประมาณระยะยาวด้านเทคโนโลยี (ICT Strategic Budget Plan)	เพื่อความต่อเนื่องในการพัฒนาและบำรุงรักษาระบบ	ลดความเสี่ยงจากการเปลี่ยนแปลงนโยบายหรืองบประมาณ
4. โครงการเสริมสร้างวัฒนธรรมข้อมูลปลอดภัยในองค์กร (Information Security Culture Program)	เพื่อส่งเสริมพฤติกรรมผู้ใช้ที่ปลอดภัย เช่น การใช้รหัสผ่าน การป้องกันข้อมูลรั่วไหล	ลดความเสี่ยงจากบุคลากรภายในและการใช้งานที่ไม่ระมัดระวัง

ดังนั้น ผลการวิเคราะห์ TOWS Matrix จากการวิเคราะห์สภาพแวดล้อม (SWOT Analysis) ช่วยให้เห็นแนวทางจัดการความเสี่ยงของคลังสารสนเทศดิจิทัลอย่างเป็นระบบ โดยเน้นพัฒนาเทคโนโลยีและความปลอดภัยข้อมูลให้ทันสมัย เสริมศักยภาพบุคลากรและสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยสารสนเทศ จัดทำนโยบายและมาตรการรองรับภัยคุกคามไซเบอร์และเหตุฉุกเฉิน รวมถึงวางแผนงบประมาณระยะยาวเพื่อความยั่งยืนของระบบ ทั้งนี้เพื่อให้คลังสารสนเทศดิจิทัลของมหาวิทยาลัยเป็นศูนย์กลางความรู้ที่ปลอดภัยและมีประสิทธิภาพสูงสุด