ผลการดำเนินงานตามแผนบริหารความเสี่ยง ด้านการทุจริตและประพฤติมิชอบ
วิทยาลัยการศึกษาตลอดชีวิต
ณ ไตรมาสที่ 4 ปีงบประมาณ พ.ศ. 2567

ลำดับ	ประเด็นความเสี่ยง	ประเภทความเสี่ยง	ระดับความเสี่ยง			
			ไตรมาสที่ 1	ไตรมาสที่ 2	ไตรมาสที่ 3	ไตรมาสที่ 4
1	การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ด้านกฎ ระเบียบ และข้อบังคับ	3 x 3 = 9 ปานกลาง	3 x 2 = 6 ต่ำ	3 x 2 = 6 ต่ำ	3 x 2 = 6 ต่ำ
2	การทุจริตในประเด็นที่เกี่ยวข้องกับสินบน	ด้านกฎ ระเบียบ และข้อบังคับ	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก

แผนบริหารความเสี่ยงวิทยาลัยการศึกษาตลอดชีวิต ประจำปีงบประมาณ พ.ศ. 2567
ประเด็นความเสี่ยงที่ 1 : การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประเภทความเสี่ยง : ด้านกฎ ระเบียบ ข้อบังคับ (Compliance Risk)

1) สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน	ปัจจัยภายนอก
1. ขาดมาตรการการปกป้องข้อมูลส่วนบุคคลที่เหมาะสม	1. หน่วยงานภายนอกไม่ปฏิบัติตามแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคล
2. ผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคลในการขาดความตระหนัก ความรู้และทักษะเกี่ยวกับการละเมิดความเป็นส่วนตัว	2. มิจฉาชีพโจรกรรมข้อมูลที่สำคัญ ผ่านกระบวนการ Hacking, Compromising หรือ Phishing เป็นต้น
3. ขาดการป้องกันการรักษาความปลอดภัยในระบบโครงสร้างพื้นฐาน (เครือข่ายและศูนย์ข้อมูล) และระบบสารสนเทศของหน่วยงาน	3. ภัยคุกคามจากมัลแวร์ ไวรัสคอมพิวเตอร์ และการโจมตีในรูปแบบอื่น ๆ
4. การนำแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลไปสู่การปฏิบัติขาดประสิทธิผล	

2) ผลกระทบของความเสี่ยงต่อหน่วยงาน

ผลกระทบของความเสี่ยง
1. ข้อมูลส่วนบุคคลของผู้เรียนถูกละเมิด ก่อให้เกิดความเสียหายของเจ้าของข้อมูลส่วนบุคคล
2. ภาพลักษณ์ของหน่วยงานเกิดความเสียหาย
3. เกิดการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง

3) ตัวชี้วัดความเสี่ยง (KRI)

<u>KRI 1</u>:

1. จำนวนเหตุละเมิดข้อมูลส่วนบุคคล
2. ระดับความเข้าใจแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคล
3. ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคล จากสำนักงานคุ้มครองข้อมูลส่วนบุคคล
4. ระดับดำเนินมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลในการทำงานของหน่วยงาน

KRI	Risk Limit (เพดานความเสี่ยง)	
	Risk Appetite (ระดับความเสี่ยงที่ยอมรับได้)	Risk Tolerance (ช่วงเบี่ยงเบนจากระดับที่ยอมรับได้)
1	L x I = 2 x 1	L x I = 2 x 2

4) เกณฑ์การประเมินระดับความเสี่ยง: โอกาสเกิดและผลกระทบ (Likelihood & Impact)

ระดับ	ผลกระทบ (I)			
	L1 **จำนวนเหตุละเมิดข้อมูลส่วนบุคคล**	**L2** **ระดับความเข้าใจแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคล**	**I1** **ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคล จากสำนักงานคุ้มครองข้อมูลส่วนบุคคล**	**I2** **ระดับดำเนินมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลในการทำงานของหน่วยงาน**
5 (สูงมาก)	เกิดเหตุละเมิดข้อมูลส่วนบุคคลมากกว่า 5 ครั้งต่อปี	ขาดนโยบายและแนวปฏิบัติ	ข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวจำนวนมากถูกละเมิด และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ส่งผลให้ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล และนำมาซึ่งการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง	ไม่มีการดำเนินมาตรการ ฯ
4 (สูง)	เกิดเหตุละเมิดข้อมูลส่วนบุคคลจำนวน 4-5 ครั้งต่อปี	มีนโยบายฯ แต่ขาดการถ่ายทอด หรือระดับความเข้าใจฯ ต่ำหรือน้อยกว่า	ข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวถูกละเมิด และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ส่งผลให้ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล และนำมาซึ่งการฟ้องร้องทั้งในคดี อาญา ปกครอง และทางแพ่ง	มีการดำเนินมาตรการ ฯ น้อย
3 (ปานกลาง)	เกิดเหตุละเมิดข้อมูลส่วนบุคคลจำนวน 2-3 ครั้งต่อปี	ระดับความเข้าใจฯ ปานกลาง	ข้อมูลส่วนบุคคลจำนวนมากถูกละเมิด แต่ไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล แต่ส่งผลให้ต้องแจ้งเหตุละเมิดไปยังสำนักงานคุ้มครองข้อมูลส่วนบุคคล	มีการดำเนินมาตรการ ฯ ปานกลาง

ระดับ	ผลกระทบ (I)			
	L1 **จำนวนเหตุละเมิดข้อมูลส่วนบุคคล**	**L2** **ระดับความเข้าใจแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคล**	**I1** **ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคล จากสำนักงานคุ้มครองข้อมูลส่วนบุคคล**	**I2** **ระดับดำเนินมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลในการทำงานของหน่วยงาน**
2 (ต่ำ)	เกิดเหตุละเมิดข้อมูลส่วนบุคคลจำนวน 1 ครั้งต่อปี	ระดับความเข้าใจฯ สูง	ข้อมูลส่วนบุคคลถูกละเมิดแต่ไม่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล และไม่ต้องแจ้งเหตุละเมิดไปยังสำงานคุ้มครองข้อมูลส่วนบุคคล	มีการดำเนินมาตรการ ฯ มาก
1 (ต่ำมาก)	ไม่เกิดเหตุละเมิดข้อมูลส่วนบุคคล	ระดับความเข้าใจฯ สูงมาก	ไม่ได้รับผลกระทบ	มีการดำเนินมาตรการ ฯ อย่างเข้มงวด

5) ข้อมูลประเมินระดับความเสี่ยงที่เหลืออยู่

	ความหมาย	**(Data Owner)**
L1	จำนวนเหตุละเมิดข้อมูลส่วนบุคคล	งานเทคโนโลยีสารสนเทศ
L2	ระดับความเข้าใจแนวนโยบายและมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคล	
I1	ข้อมูลที่ได้รับแจ้งเหตุละเมิดเกี่ยวกับข้อมูลส่วนบุคคล จากสำนักงานคุ้มครองข้อมูลส่วนบุคคล	
I2	ระดับดำเนินมาตรการการรักษาความปลอดภัยข้อมูลส่วนบุคคลในการทำงานของหน่วยงาน	

การประเมินระดับความเสี่ยง

ประเด็นความเสี่ยง	**ประเภทความเสี่ยง**	**ระดับความเสี่ยง**			
		ไตรมาสที่1	**ไตรมาสที่2**	**ไตรมาสที่3**	**ไตรมาสที่4**
การดำเนินการที่ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	ด้านกฎ ระเบียบ และข้อบังคับ	3 x 3 = 9 ปานกลาง	3 x 2 = 6 ต่ำ	3 x 2 = 6 ต่ำ	3 x 2 = 6 ต่ำ

6) ผลการดำเนินงานตามมาตรการควบคุมความเสี่ยง

มาตรการควบคุมความเสี่ยง	สรุปผลการดำเนินงานที่สำคัญ
1. จัดทำมาตรการ และแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคล รวมถึงการทบทวนมาตรการและแนวปฏิบัติอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง	1. มาตรการในการลงทะเบียนผู้เรียน มีการอธิบายและการยินยอม/ไม่ยินยอมข้อมูลส่วนบุคคล 2. ผู้เรียนสามารถทำการยอมรับ/ยกเลิก ข้อมูลส่วนบุคคล ได้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 3. มาตรการเปิดเผยขอมูลลูกค้าแก่บุคคลที่สาม โดยการทำเอกสารลายลักษณ์อักษรเพื่อลงนามอย่างชัดเจน สำหรับหน่วยงานอื่นหรือบริษัทเอกชนที่มีการประสานความร่วมมือในส่วนข้อมูลผู้เรียน
2. พัฒนาความรู้ของบุคลากร ทั้งผู้ใช้ข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ให้เกิดการตระหนัก มีความรู้ และทักษะในการจัดการข้อมูลส่วนบุคคล	1. ให้เจ้าหน้าที่เข้าร่วมการอบรมความรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3. พัฒนาสถาปัตยกรรม ขององค์กร (EA: Enterprise Architecture) ที่รองรับ ROPA (Record of Processing Activity) เพื่อให้สามารถพิจารณาความเชื่อมโยงของระบบและข้อมูลได้ และสามารถตอบสนองได้หากเกิดการละเมิดข้อมูลส่วนบุคคลขึ้น	1. ดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ระบุไว้ในมาตรา 39 เกี่ยวกับการจัดทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้ 1.1 วัตถุประสงค์ของการเก็บรวมรวมข้อมูลส่วนบุคคล 1.2 การปฏิเสธคำขอหรือการคัดค้านการใช้ข้อมูลส่วนบุคคล
4. จัดให้มีการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคลขึ้นอย่างน้อย 1 ครั้งต่อปี	อยู่ระหว่างการออกแบบและวางแนวทางการซ้อมกระบวนการตอบสนองในกรณีเกิดการละเมิดข้อมูลส่วนบุคคล

แผนบริหารความเสี่ยงวิทยาลัยการศึกษาตลอดชีวิต ประจำปีงบประมาณ พ.ศ. 2567
ประเด็นความเสี่ยง 2 การทุจริตในประเด็นที่เกี่ยวข้องกับสินบน

ประเภทความเสี่ยง: ด้านกฎ ระเบียบ และข้อบังคับ(Compliance Risk)

ตารางที่ 1 สาเหตุหลักจากปัจจัยภายในและปัจจัยภายนอกที่นำไปสู่ความเสี่ยง

ปัจจัยภายใน	ปัจจัยภายนอก
1. ด้านการใช้อำนาจตามกฎหมาย/ การให้บริการตามภารกิจ 1.1 การใช้อำนาจหน้าที่เรียกรับผลประโยชน์หรือสินบน เพื่อแลกกับการปฏิบัติงานหรือบริการจากผู้เรียน ผู้รับบริการ ประชาชน หรือผู้ซึ่งอาจได้รับประโยชน์จากการปฏิบัติหน้าที่นั้น	1. ด้านการใช้อำนาจตามกฎหมาย/ การให้บริการตามภารกิจ 1.1 บุคคลภายนอกเสนอผลประโยชน์หรือสินบนให้ผู้ปฏิบัติงาน เอื้อประโยชน์ในการบริการตามที่บุคคลนั้นต้องการ
2. ด้านการจัดซื้อจัดจ้าง 2.1 การเรียกรับผลประโยชน์หรือสินบนจากผู้เสนอราคา/ผู้รับจ้าง เพื่อแลกกับการกำหนดคุณสมบัติการจ้างเพื่อเอื้อประโยชน์ให้กับผู้เสนอราคา/ผู้รับจ้าง 2.2 การเรียกรับผลประโยชน์หรือสินบน เพื่อแลกกับข้อมูลภายในของหน่วยงาน อันเป็นประโยชน์ต่อการเสนอราคา นำไปสู่โอกาสชนะการประกวดราคางานจ้างนั้น ๆ	2. ด้านการจัดซื้อจัดจ้าง 2.1 ผู้เสนอราคา/ผู้รับจ้าง เสนอผลประโยชน์หรือสินบน แลกกับการกำหนดคุณสมบัติการจ้าง 2.2 ผู้เสนอราคา/ผู้รับจ้าง เสนอผลประโยชน์หรือสินบนเพื่อแลกกับข้อมูลภายในของหน่วยงาน อันเป็นประโยชน์ต่อการเสนอราคา
3. ด้านการบริหารงานบุคคล 3.1 การเรียกรับผลประโยชน์หรือสินบนจากผู้สมัครงาน เพื่อเอื้อประโยชน์ในการรับคัดเลือกเข้าทำงาน 3.2 การเรียกรับผลประโยชน์หรือสินบนจากผู้สมัครงาน เพื่อเอื้อประโยชน์หรือแลกกับความก้าวหน้าในการทำงาน	3. ด้านการบริหารงานบุคคล 3.1 บุคคลภายนอก/ผู้สมัคร เสนอผลประโยชน์หรือสินบน เพื่อเอื้อประโยชน์ในการรับคัดเลือกเข้าทำงาน 3.2 บุคลากรในส่วนงาน เสนอผลประโยชน์หรือสินบน แลกกับความก้าวหน้าในการทำงาน

ตารางที่ 2 ผลกระทบของความเสี่ยงต่อหน่วยงาน

ผลกระทบของความเสี่ยง
1. ผลกระทบต่อระดับความโปร่งใส ชื่อเสียง และความเชื่อมั่นต่อวิทยาลัย รวมถึงภาพลักษณ์ของมหาวิทยาลัย

ตารางที่ 3 การกำหนดตัวชี้วัดความเสี่ยง/ตัวบ่งชี้ความเสี่ยง/สัญญาณเตือนภัย (KRI)

KRI 1: จำนวนการสอบสวนความผิดการทุจริตในประเด็นที่เกี่ยวข้องกับสินบน

KRI	Risk Limit (เพดานความเสี่ยง)	
	Risk Appetite (ระดับความเสี่ยงที่ยอมรับได้)	Risk Tolerance (ช่วงเบี่ยงเบนจากระดับที่ยอมรับได้)
1	L x I = 1 x 1	L x I = 1 x 1

ตารางที่ 4 ระดับโอกาสที่จะเกิดความเสี่ยง (ค่า L : Likelihood)

ระดับ	จำนวนครั้งการรับสินบน
5	มีโอกาสเกิดการเรียกรับสินบนจำนวนมากกว่า 1 ครั้งในรอบ 1 ปี
4	มีโอกาสเกิดการเรียกรับสินบนจำนวน 1 ครั้งในรอบ 1 ปี
3	มีโอกาสเกิดการเรียกรับสินบนจำนวน 1 ครั้งในรอบ 3 ปี
2	มีโอกาสเกิดการเรียกรับสินบนจำนวน 1 ครั้งในรอบ 5 ปี
1	ไม่เกิดกรณีการเรียกรับสินบน

ตารางที่ 5 ระดับผลกระทบ/ความรุนแรงหากเกิดความเสี่ยง (ค่า I : Impact)

ระดับ	ด้านชื่อเสียง
5	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและมหาวิทยาลัย
4	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและส่วนงาน
3	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคลและหน่วยงาน
2	เกิดความเสียหายด้านชื่อเสียงในระดับบุคคล
1	ไม่มีการเสียชื่อเสียง

การประเมินระดับความเสี่ยง

ประเด็นความเสี่ยง	ประเภทความเสี่ยง	ระดับความเสี่ยง			
		ไตรมาสที่1	ไตรมาสที่2	ไตรมาสที่3	ไตรมาสที่4
การทุจริตในประเด็นที่เกี่ยวข้องกับสินบน	ด้านกฎ ระเบียบ และข้อบังคับ	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก	1 x 1 = 1 ต่ำมาก

6) ผลการดำเนินงานตามมาตรการควบคุมความเสี่ยง

มาตรการควบคุมความเสี่ยง	สรุปผลการดำเนินงานที่สำคัญ
1. อบรมสัมมนา/ให้ความรู้เกี่ยวกับจริยธรรมการปฏิบัติงาน	1. เผยแพร่แนวปฏิบัติ Dos & Don'ts ของวิทยาลัยการศึกษาตลอดชีวิต 2.. อบรมแนวทางการขออนุมัติปฏิบัติงานนอกเวลาทำการและการเบิกจ่ายค่าตอบแทนปฏิบัติงานนอกเวลาทำการ 3. อบรมแนวปฏิบัติการจัดกิจกรรม ประชุม อบรม สัมมนา การเดินทางไปปฏิบัติงาน และการชดใช้เงินยืมทดรองจ่ายตามระยะเวลาที่กำหนด 4. อบรมแนวทางประมาณการค่าใช้จ่ายในการจัดกิจกรรม ประชุม อบรม สัมมนา การเดินทางไปปฏิบัติงาน 5. อบรมแนวปฏิบัติการดำเนินการจัดหาพัสดุฯ (ว 119)
2. เพิ่มมาตรการควบคุมภายในและใช้เทคโนโลยีในการตรวจสอบการปฏิบัติงานของผู้ปฏิบัติงาน	กำหนดสิทธิ์การเข้าถึงการใช้งานข้อมูลในระบบหลังบ้านเว็บไซต์ของวิทยาลัยการศึกษาตลอดชีวิต
3. มีระบบตักเตือน ลงโทษที่เหมาะสม	กำหนดบทลงโทษและตักเตือนบุคลากรทางด้านการดำเนินเอกสารด้านสารบรรณ การเงิน และพัสดุ
4. ส่งเสริมการสร้างจิตสำนึกด้านจริยธรรมและความโปร่งใส (ITA)	1.จัดตั้งคณะทำงานที่ปรึกษาด้านจริยธรรมองค์กร 2.จัดตั้งคณะทำงานส่งเสริมและขับเคลื่อนวัตนธรรมองค์กร เพื่อดำเนินกิจกรรมที่มีวัตถุประสงค์เพื่อสร้างจิตสำนึกด้านจริยธรรมและความโปร่งใส โดยการดำเนินกิจกรรม เช่น 1. กิจกรรม LE Sharing เรื่อง การจัดทำเอกสารเพื่อเปิดเผยข้อมูลสาธารณะ 2. . กิจกรรม LE Sharing เรื่อง การขับเคลื่อนองค์กรด้วยการบริหารจัดการข้อมูลอย่างโปรงใส