**การประเมินความเสี่ยงการทุจริต และประพฤติมิชอบ ประจำปีงบประมาณ 2565**

**การประเมินความเสี่ยงการทุจริต และประพฤติมิชอบ (เลือกการประเมินด้านที่ 1 )**

**🗹** 1. ความเสี่ยงการทุจริตที่เกี่ยวข้องกับการพิจารณอนุมัติ อนุญาต

🞎 2. ความเสี่ยงการทุจริตในความโปร่งใสของการใช้อำนาจและตำแหน่งหน้าที่

🞎 3. ความเสี่ยงการทุจริตในความโปร่งใสของการใช้จ่ายงบประมาณและการบริหารจัดการทรัพยากรภาครัฐ

**ตารางที่ 1 ตารางระบุความเสี่ยง (Known Factor และ Unknown Factor)**

|  |  |  |
| --- | --- | --- |
| **โอกาส/ความเสี่ยงการทุจริต** | **ประเภทความเสี่ยง** | |
| **Known Factor** | **Unknown Factor** |
| 1. บุคลากรภายในองค์กรปฏิบัติงานไม่เป็นไปตามระเบียบข้อบังคับ มีเจตนากระทำการที่ส่อไปในทางทุจริตเพื่อผลประโยชน์ต่อตนเองหรือร่วมรู้เห็นเป็นใจกับบุคคลภายนอกที่ประสงค์ร้ายต่อองค์กร สร้างความเสียหายในด้านการเงินกระทบต่อความน่าเชื่อถือและชื่อเสียงในภาพรวม |  | **√** |
| 2. กระบวนการปฏิบัติงานที่ไม่เป็นไปตามแนวปฏิบัติของหน่วยงานกำกับควบคุมรวมถึงการกำหนดจุดควบคุมไม่เพียงพอก่อให้เกิดช่องโหว่ เกิดความเสี่ยงที่บุคลากรภายในทำการทุจริตสร้างความเสียหายต่อองค์กร เช่น การถูกเปรียบเทียบปรับหรือถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมายส่งผลกระทบต่อภาพลักษณ์ขององค์กร |  | **√** |
| 3. ภัยคุกคามทาง Cyber จากบุคคลภายนอกที่ไม่ประสงค์ดีต่อองค์กร ตลอดจนระบบเทคโนโลยีสารสนเทศไม่พร้อมใช้งานขาดการควบคุมการเข้าถึงระบบงานการรักษาความปลอดภัยที่รัดกุมไม่ก่อให้เกิดความเสี่ยงทั้งจากบุคลากรภายในและบุคลากรภายนอกใช้ในการทุจริต ในการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บในระบบฐานข้อมูลส่งผลต่อความเสียหายต่อองค์กร |  | **√** |

**คำอธิบาย :** ตารางที่ 1 อธิบายรายละเอียดความเสี่ยงการทุจริต เช่น รูปแบบ พฤติการณ์การทุจริตที่มความเสี่ยงเท่านั้น และควรอธิบายพฤติการณ์ความเสี่ยงให้ละเอียด ชัดเจน มากที่สุด

- ความเสี่ยงที่เคยเกิดหรือคาดว่าจะเกิดขึ้นสุงมีประวัติอยู่แล้ว ให้ใส่เครื่องหมาย √ ในช่องKnown Factor

- ความเสี่ยงที่ไม่เคยเกิดขึ้นหรือไม่มีประวัติมาก่อน แต่มีความเสี่ยงจากการพยากรณ์ ในอนาคตให้ใส่เครื่องหมาย √ ในช่อง Unknown Factor

- หน่วยงานสามารถปรับแบบได้โดยไม่ระบุว่าเป็นประเภท Known Factor หรือ Unknown Factor

**ตารางที่ 2 ตารางแสดงสถานะความเสี่ยง (แยกตามรายสีไฟจราจร)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ที่** | **โอกาส/ความเสี่ยงการทุจริต** | **เขียว** | **เหลือง** | **ส้ม** | **แดง** |
| 1 | บุคลากรภายในองค์กรปฏิบัติงานไม่เป็นไปตามระเบียบข้อบังคับ มีเจตนากระทำการที่ส่อไปในทางทุจริตเพื่อผลประโยชน์ต่อตนเองหรือร่วมรู้เห็นเป็นใจกับบุคคลภายนอกที่ประสงค์ร้ายต่อองค์สร้างความเสียหายในด้านการเงินกระทบต่อความน่าเชื่อถือและชื่อเสี่ยงในภาพรวม |  | √ |  |  |
| 2 | กระบวนการปฏิบัติงานที่ไม่เป็นไปตามแนวปฏิบัติของหน่วยงานกำกับควบคุมรวมถึงการกำหนดจุดควบคุมไม่เพียงพอก่อให้เกิดช่องโหว่ เกิดความเสี่ยงที่บุคลากรภายในทำการทุจริตสร้างความเสียหายต่อองค์กร เช่น การถูกเปรียบเทียบปรับหรือถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมายส่งผลกระทบต่อภาพลักษณ์ขององค์กร |  | √ |  |  |
| 3 | ภัยคุกคามทาง Cyber จากบุคคลภายนอกที่ไม่ประสงค์ดีต่อองค์กร ตลอดจนระบบเทคโนโลยีสารสนเทศไม่พร้อมใช้งานขาดการควบคุมการเข้าถึงระบบงานการรักษาความปลอดภัยที่รัดกุมไม่ก่อให้เกิดความเสี่ยงทั้งจากบุคลากรภายในและบุคลากรภายนอกใช้ในการทุจริต ในการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บในระบบฐานข้อมูลส่งผลต่อความเสียหายต่อองค์กร |  | √ |  |  |

**คำอธิบาย :** ความหมายของสถานะความเสี่ยงตามสีไฟจราจรมีรายละเอียดดังนี้

* **สถานะสีเขียว :** ความเสี่ยงระดับต่ำ
* **สถานะสีเหลือง :** ความเสี่ยงระดับปานกลางและสามารถใช้ความรอบคอบระมัดระวังในระหว่างปฏิบัติงานตามปกติควบคุมดูแลได้
* **สถานะสีส้ม :** ความเสี่ยงระดับสูงเป็นกระบวนงานที่มีผู้เกี่ยวข้องหลายคนหลายหน่วยงานภายในองค์กรมีหลายขั้นต้อนจนยากต่อการควบคุมหรือไม่มีอำนาจควบคุมข้ามหน่วยงานตามหน้าที่ปกติ
* **สถานะสีแดง :** ความเสี่ยงระดับสูงมากเป็นกระบวนงานที่เกี่ยวข้องกับบุคคลภายนอกคนที่ไม่รู้จักไม่สามารถตรวจสอบได้ชัดเจนสามารถกำกับติดตามได้อย่างใกล้ชิดหรืออย่างสม่ำเสมอ

**ตารางที่ 3 ตารรางเมทริกส์ระดับความเสี่ยง (Risklevel matrix)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ที่** | **โอกาส/ความเสี่ยงการทุจริต** | **ระดับความจำเป็นของการเข้าระวัง** | | | **ระดับความรุนแรงของผลกระทบ** | | | **ค่าความเสี่ยงจำเป็น x รุนแรง** |
| **3** | **2** | **1** | **3** | **2** | **1** |
| 1 | บุคลากรภายในองค์กรปฏิบัติงานไม่เป็นไปตามระเบียบข้อบังคับ มีเจตนากระทำการที่ส่อไปในทางทุจริตเพื่อผลประโยชน์ต่อตนเองหรือร่วมรู้เห็นเป็นใจกับบุคคลภายนอกที่ประสงค์ร้ายต่อองค์สร้างความเสียหายในด้านการเงินกระทบต่อความน่าเชื่อถือและชื่อเสี่ยงในภาพรวม |  | 2 |  |  | 2 |  | 4 |
| 2 | กระบวนการปฏิบัติงานที่ไม่เป็นไปตามแนวปฏิบัติของหน่วยงานกำกับควบคุมรวมถึงการกำหนดจุดควบคุมไม่เพียงพอก่อให้เกิดช่องโหว่ เกิดความเสี่ยงที่บุคลากรภายในทำการทุจริตสร้างความเสียหายต่อองค์กร เช่น การถูกเปรียบเทียบปรับหรือถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมายส่งผลกระทบต่อภาพลักษณ์ขององค์กร |  | 2 |  |  | 2 |  | 4 |
| 3 | ภัยคุกคามทาง Cyber จากบุคคลภายนอกที่ไม่ประสงค์ดีต่อองค์กร ตลอดจนระบบเทคโนโลยีสารสนเทศไม่พร้อมใช้งานขาดการควบคุมการเข้าถึงระบบงานการรักษาความปลอดภัยที่รัดกุมไม่ก่อให้เกิดความเสี่ยงทั้งจากบุคลากรภายในและบุคลากรภายนอกใช้ในการทุจริต ในการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บในระบบฐานข้อมูลส่งผลต่อความเสียหายต่อองค์กร |  | 2 |  |  | 2 |  | 4 |

**คำอธิบาย :** ตารางที่ 3 ข้อมูลที่มีสถานะความเสี่ยงในช่องสีส้มและสีแดงจากตารางที่ 2 มาหาค่าความเสี่ยงรวม (ระดับความจำเป็นของการเฝ้าระวัง คูณ ระดับความรุนแรงของผลกระทบ)

**ตารางที่ 4 ตารางแสดงการประเมินการควบคุมความเสี่ยง**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **โอกาส/ความเสี่ยงการทุจริต** | **คุณภาพการจัดการ** | **ค่าประเมินการควบคุมความเสี่ยงการทุจริต** | | |
| **ค่าความเสี่ยงระดับต่ำ** | **ค่าความเสี่ยงระดับปานกลาง** | **ค่าความเสี่ยงระดับสูง** |
| 1. บุคลากรภายในองค์กรปฏิบัติงานไม่เป็นไปตามระเบียบข้อบังคับ มีเจตนากระทำการที่ส่อไปในทางทุจริตเพื่อผลประโยชน์ต่อตนเองหรือร่วมรู้เห็นเป็นใจกับบุคคลภายนอกที่ประสงค์ร้ายต่อองค์สร้างความเสียหายในด้านการเงินกระทบต่อความน่าเชื่อถือและชื่อเสี่ยงในภาพรวม | **ดี** | **ต่ำ** | **ค่อนข้างต่ำ** | **ปานกลาง** |
| **พอใช้** | **ค่อนข้างต่ำ** | **ปานกลาง** | **ค่อนข้างสูง** |
| **อ่อน** | **ปานกลาง** | **ค่อนข้างสูง** | **สูง** |
| 2. กระบวนการปฏิบัติงานที่ไม่เป็นไปตามแนวปฏิบัติของหน่วยงานกำกับควบคุมรวมถึงการกำหนดจุดควบคุมไม่เพียงพอก่อให้เกิดช่องโหว่ เกิดความเสี่ยงที่บุคลากรภายในทำการทุจริตสร้างความเสียหายต่อองค์กร เช่น การถูกเปรียบเทียบปรับหรือถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมายส่งผลกระทบต่อภาพลักษณ์ขององค์กร | **ดี** | **ต่ำ** | **ค่อนข้างต่ำ** | **ปานกลาง** |
| **พอใช้** | **ค่อนข้างต่ำ** | **ปานกลาง** | **ค่อนข้างสูง** |
| **อ่อน** | **ปานกลาง** | **ค่อนข้างสูง** | **สูง** |
| 3. ภัยคุกคามทาง Cyber จากบุคคลภายนอกที่ไม่ประสงค์ดีต่อองค์กร ตลอดจนระบบเทคโนโลยีสารสนเทศไม่พร้อมใช้งานขาดการควบคุมการเข้าถึงระบบงานการรักษาความปลอดภัยที่รัดกุมไม่ก่อให้เกิดความเสี่ยงทั้งจากบุคลากรภายในและบุคลากรภายนอกใช้ในการทุจริต ในการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บในระบบฐานข้อมูลส่งผลต่อความเสียหายต่อองค์กร | **ดี** | **ต่ำ** | **ค่อนข้างต่ำ** | **ปานกลาง** |
| **พอใช้** | **ค่อนข้างต่ำ** | **ปานกลาง** | **ค่อนข้างสูง** |
| **อ่อน** | **ปานกลาง** | **ค่อนข้างสูง** | **สูง** |

**คำอธิบาย :** ตารางที่ 4 ให้นำค่าความเสี่ยงรวม (จำเป็น x รุนแรง) จากตารางที่ 3 มาทำการประเมินการควบคุมความเสี่ยงการทุจริตโดยการวิเคราะห์จากคุณภาพการจัดการขององค์กรกับความเสี่ยงเรื่องที่ทำการประเมิน (ดี / พอใช้ / อ่อน)เพื่อประเมินว่าความเสี่ยงการทุจริตมีค่าความเสี่ยงอยู่ระดับใดจะได้นำไปบริหารจัดการความเสี่ยงตามความรุนแรงของความเสี่ยง

**ตารางที่ 5 แผนบริหารความเสี่ยง**

**แผนบริหารความเสี่ยงเพื่อป้องกันการทุจริต**

|  |  |  |
| --- | --- | --- |
| **ที่** | **รูปแบบ พฤติการณ์ความเสี่ยงการทุจริต** | **มาตรการป้องกันการทุจริต** |
| 1 | บุคลากรภายในองค์กรปฏิบัติงานไม่เป็นไปตามระเบียบข้อบังคับ มีเจตนากระทำการที่ส่อไปในทางทุจริตเพื่อผลประโยชน์ต่อตนเองหรือร่วมรู้เห็นเป็นใจกับบุคคลภายนอกที่ประสงค์ร้ายต่อองค์สร้างความเสียหายในด้านการเงินกระทบต่อความน่าเชื่อถือและชื่อเสี่ยงในภาพรวม | 1. กำกับดูแลและติดตามให้เจ้าหน้าที่มีการปฏิบัติ โดยมีกลไกการถ่วงดุลและมีการควบคุม กำกับ ตรวจสอบที่มีประสิทธิภาพเป็นไปตามหลักการควบคุมภายในทั่วองค์กร |
| 2 | กระบวนการปฏิบัติงานที่ไม่เป็นไปตามแนวปฏิบัติของหน่วยงานกำกับควบคุมรวมถึงการกำหนดจุดควบคุมไม่เพียงพอก่อให้เกิดช่องโหว่ เกิดความเสี่ยงที่บุคลากรภายในทำการทุจริตสร้างความเสียหายต่อองค์กร เช่น การถูกเปรียบเทียบปรับหรือถูกฟ้องร้องจากการไม่ปฏิบัติตามกฎหมายส่งผลกระทบต่อภาพลักษณ์ขององค์กร |
| 3 | ภัยคุกคามทาง Cyber จากบุคคลภายนอกที่ไม่ประสงค์ดีต่อองค์กร ตลอดจนระบบเทคโนโลยีสารสนเทศไม่พร้อมใช้งานขาดการควบคุมการเข้าถึงระบบงานการรักษาความปลอดภัยที่รัดกุมไม่ก่อให้เกิดความเสี่ยงทั้งจากบุคลากรภายในและบุคลากรภายนอกใช้ในการทุจริต ในการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่จัดเก็บในระบบฐานข้อมูลส่งผลต่อความเสียหายต่อองค์กร | 2. การปฏิบัติงานในระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น เจ้าหน้าที่จะต้องมีรหัสผู้ใช้งานและรหัสผ่าน (Username และ Password) ให้หัวหน้าหน่วยงานคลังควบคุมดูแลการใช้รหัสผู้ใช้งานของเจ้าหน้าที่ในการนำเข้าข้อมูลและการแก้ไขข้อมูลของเจ้าหน้าที่ ทั้งนี้ รหัสผู้ใช้งานให้ถือเป็นความลับ เจ้าของรหัสผู้ใช้งานต้องรับผิดชอบผลเสียหายอันเกิดจากการใช้งานนั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการประทำของผู้อื่น |
| 4 | พนักงานอาจจะมีความขัดแย้งทางผลประโยชน์  (Conflict of Interest) | 3. นโยบายการขัดกันระหว่างประโยชน์ส่วนบุคคลและประโยชน์ส่วนร่วมขององค์กร |

**คำอธิบาย :** ตารางที่ 5 พิจารณาเหตุการณ์ความเสี่ยงที่มีค่าความเสี่ยงการทุจริตจากตารางที่ 4 ตามลำดับ ความรุนแรงความเสี่ยงที่อยู่ในระดับสูงค่อนข้างสูงปานกลาง มาจัดทำแผนบริหารความเสี่ยงเพื่อป้องกันการทุจริต ต่อไป