

## แบบฟอร์มการประเมินตนเอง เพื่อการป้องกันและปราบปรามการทุจริตมหาวิทยาลัยเทคโนโลยีสุรนารี

หน่วยงาน :ศูนย์คอมพิวเตอร์ -ฝ่ายโครงสร้างพื้นฐานและบริการงานคอมพิวเตอร์

แบบ C-1

| งานหลัก   | งานย่อย   | เหตุการณ์หลัก  | เหตุการณ์สุ่มเสี่ยง   | <input checked="" type="checkbox"/> เลือกตัวเลือกที่ตรงกับหน่วยงานของท่าน |
|---|---|--|---|---|
| <b>งานหลัก :</b><br>1. งานบริการระบบ internet data Center | <b>งานย่อย :</b><br>1. งานดูแลระบบสารสนเทศ<br>2. งานดูแลระบบบัญชีผู้ใช้งานส่วนกลางมหาวิทยาลัย | 1. การยักยอก (Asset Misappropriation Fraud)            | 1.1 ปลอมแปลงเอกสารเบิกเงิน                                  |   |
|   |   |  | 1.2 เบิกค่าใช้จ่ายสูงเกินจริง                               |   |
|   |   |  | 1.3 เซ็นต์รับงานที่ยังไม่เสร็จ                              |   |
|   |   |  | 1.4 จ่ายเงินเดือน / ค่าแรงให้พนักงานที่ไม่มีตัวตน           |   |
|   |   |  | 1.5 นำเอกสารมาเบิกเงินซ้ำ                                   |   |
|   |   |  | 1.6 ปลอมแปลงลายเซ็นผู้อนุมัติจ่ายเงิน                       |   |
|   |   |  | 1.7 ขายเป็นเงินสดแต่บันทึกเป็นลูกหนี้ นำเงินสดเข้ากระเป๋า   |   |
|   |   |  | 1.8 นำเงินสดย่อยไปหมุนใช้ส่วนตัว                            |   |
|   |   |  | 1.9 อื่นๆ โปรดระบุ.....                                     |   |
|   |   | 2. ทุจริตด้านจัดซื้อ (Procurement Fraud)               | 2.1 มีความสัมพันธ์ส่วนตัวกับผู้ขาย                          |   |
|   |   |  | 2.2 ผู้ขายที่เสนอราคาไม่มีตัวตนจริง                         |   |
|   |   |  | 2.3 ราคาขาย/ค่าบริการของผู้ขายสูงเกินจริงและสูงกว่าราคาตลาด |   |
|   |   |  | 2.4 อื่นๆ โปรดระบุ.....                                     |   |
|   |   | 3. การติดสินบน และการคอร์รัปชัน (Bribery & Corruption) | 3.1 การติดสินบน   |   |
|   |   |  | 3.2 การให้หรือรับเงินใต้โต๊ะ                                |   |
|   |   |  | 3.3 การคอร์รัปชัน   |   |
|   |   |  | 3.4 การกรรโชกทรัพย์   |   |
|   |   |  | 3.5 การหลอกลวง  |   |
|   |   |  | 3.6 การสมรู้ร่วมคิด   |   |
|   |   |  | 3.7 การฟอกเงิน  |   |
|   |   |  | 3.8 อื่นๆ โปรดระบุ.....                                     |   |

| งานหลัก | งานย่อย | เหตุการณ์หลัก   | เหตุการณ์สุ่มเสี่ยง   | <input checked="" type="checkbox"/> เลือกตัวเลือกที่ตรงกับหน่วยงานของท่าน |
|---------|---------|---|---|---|
|         |         | 4. อาชญากรรมทางไซเบอร์ (Cyber Crime)                          | 4.1 การแฮกเข้าสู่ระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลส่วนบุคคล   | ✓   |
|         |         |   | 4.2 การนำ User / Password ของผู้อื่นไปใช้เพื่อประโยชน์ส่วนตัว |   |
|         |         |   | 4.3 อื่นๆ โปรดระบุ.....                                       |   |
|         |         | 5. Fraudulent Financial Reporting (การตกแต่งรายงานทางการเงิน) | 5.1 รับรู้รายได้ไม่ถูกต้อง                                    |   |
|         |         |   | 5.2 รับรู้รายการบัญชีไม่ถูกหมวดบัญชี                          |   |
|         |         |   | 5.3 ไม่รับรู้หนี้สินที่เกิดขึ้น                               |   |
|         |         |   | 5.4 ไม่รับรู้ค่าใช้จ่ายที่เกิดขึ้น                            |   |
|         |         |   | 5.5 บันทึกบัญชีผิดพลาด  |   |
|         |         |   | 5.6 ประเมินทรัพย์สินไม่เหมาะสม (อายุการใช้งาน มูลค่าซาก)      |   |
|         |         |   | 5.7 อื่นๆ โปรดระบุ.....                                       |   |

★ ข้อเสนอแนะในการจัดทำ แบบ C-1 :

- 1) งานหลักและงานย่อย คืองานตามภารกิจหรือพันธกิจของหน่วยงานและต้องระบุรายละเอียดลงไปกับลงมือปฏิบัติการ
- 2) เหตุการณ์หลัก คือ การเลือกเหตุการณ์จากแนวคิด 5 ประเภทการทุจริตและความเสี่ยงที่จะเกิดการทุจริต
- 3) เลือกเหตุการณ์สุ่มเสี่ยงที่สอดคล้องกับพันธกิจและกระบวนการปฏิบัติงานของหน่วยงานของท่าน แล้วนำเหตุการณ์สุ่มเสี่ยงที่เลือกไปจัดทำกิจกรรมควบคุมตามแบบฟอร์ม C-2 ต่อไป



★ **ข้อเสนอแนะในการทำแบบ C-2** : รายละเอียดตาม “เล่มคู่มือการกำหนดกลยุทธ์และมาตรการในการป้องกันการทุจริตระดับหน่วยงาน” หน้า 9 – 17

(สามารถดาวน์โหลดคู่มือได้ที่ <https://drive.google.com/file/d/1R0fm7VLa1mEYif3BgVxNznhRL5fADG51/view?usp=sharing>

หรือสแกน QR Code)



แบบฟอร์มรายละเอียดการกำหนดกิจกรรมรายเดือนเพื่อการป้องกันและปราบปรามการทุจริต

แบบ C-3

| กิจกรรมควบคุม  | การดำเนินการตามกิจกรรมควบคุม |      |      |      |      |       |       |      |       |      |      |      | รายละเอียดการดำเนินงาน<br>(โปรดระบุ) |                 |
|--|------------------------------|------|------|------|------|-------|-------|------|-------|------|------|------|--------------------------------------|-----------------|
|  | ต.ค.                         | พ.ย. | ธ.ค. | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. |                                      |                 |
| 1. มีการเฝ้าระวังและตรวจสอบระบบสารสนเทศอยู่เสมอ  | 100                          | 100  | 100  | 100  | 100  | 100   | 100   | 100  | 100   | 100  | 100  | 100  | 100                                  | (โปรดระบุ)..... |
| 2. ต่อ license อุปกรณ์ป้องกัน และเฝ้าระวังความปลอดภัยระบบเครือข่าย ประกอบด้วย firewall mail gateway, network monitor , จัดหา antivirus สำหรับเครื่องคอมพิวเตอร์แม่ข่าย | 100                          | 100  | 100  | 100  | 100  | 100   | 100   | 100  | 100   | 100  | 100  | 100  | 100                                  |                 |

★ ข้อแนะนำในการจัดทำ แบบ C-3 :

- นำกิจกรรมควบคุมจากแบบฟอร์ม C-2 มาวางแผนการดำเนินงาน
- กำหนดรายละเอียดการดำเนินงานตามกิจกรรมควบคุมที่กำหนดขึ้น และเพื่อใช้ในการรายงานผลการดำเนินงานให้กับมหาวิทยาลัยทราบต่อไป