<u>เอกสารที่ต้องเตรียมเพื่อการประเมินความมั่นคงปลอดภัยไซเบอร์</u>

<u>ตาม พ.ร.บ.ไซเบอร์ 2562</u>

1. จัดทำรายการทะเบียนทรัพย์สิน (Inventory)
2. จัดทำรายการทะเบียนความเสี่ยง
3. จัดทำรายการช่องโหว่ของบริการ
4. ดำเนินการประเมินช่องโหว่ของบริการ
5. ดำเนินการทดสอบเจาะระบบ (Penetration Testing)
6. จัดทำนโยบายการการควบคุมการเข้าถึง
7. จัดทำนโยบายด้านความมั่งคงปลอดภัยขั้นต่ำ
8. จัดทำนโยบายการจัดการสื่อเก็บข้อมูลแบบถอดได้
9. จัดทำนโยบายการการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
10. จัดทำนโยบายการแบ่งปันข้อมูล
11. การประเมินความเสี่ยง
12. กำาหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
13. จัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
14. การจัดการความเสี่ยง
15. การติดตามและทบทวนความเสี่ยง
16. การรายงานความเสี่ยง
17. กระบวนการการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)
18. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
19. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
20. การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)
21. แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)
22. แต่งตั้งมีผู้รับผิดชอบด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ