

แบบสอบถาม เรื่อง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่น

ความเป็นมา

เนื่องจากปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญต่อการดำเนินการขององค์กรต่าง ๆ หน่วยงานของรัฐมีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการบริหารจัดการองค์กร และให้บริการประชาชนได้อย่างทั่วถึง สะดวกและรวดเร็ว ซึ่งเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ องค์กรปกครองส่วนท้องถิ่นก็นำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการบริหารจัดการองค์กรและให้บริการประชาชนเช่นเดียวกับส่วนราชการอื่น ๆ

วัตถุประสงค์

เพื่อศึกษาการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่น และนำผลการศึกษาที่ได้ไปจัดทำข้อเสนอแนะแนวทางการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่นให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศระดับพื้นฐานภายใต้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงแนวทางการพัฒนาศักยภาพบุคลากรขององค์กรปกครองส่วนท้องถิ่นด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

คำนิยามที่เกี่ยวข้อง

ระบบสารสนเทศ หมายถึง ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญ ในสาขาทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูล เพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ หมายถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่องรู้โดยมิชอบ

ทรัพย์สินสารสนเทศ หมายถึง 1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

คำชี้แจง

1. แบบสอบถามฉบับนี้ แบ่งออกเป็น 4 ส่วน คือ
 - ส่วนที่ 1 ข้อมูลทั่วไปเกี่ยวกับระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่น
 - ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
 - ส่วนที่ 3 การพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
 - ส่วนที่ 4 ข้อเสนอแนะที่ต้องการได้รับการสนับสนุนจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
2. เนื่องจากข้อมูลดังกล่าวมีความสำคัญอย่างยิ่งต่อการดำเนินงานพัฒนาระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่นให้มีความมั่นคงปลอดภัย สามารถทำงานได้อย่างต่อเนื่อง และข้อมูลสารสนเทศมีความน่าเชื่อถือ จึงใคร่ขอความกรุณาตอบแบบสอบถามให้ครบทุกข้อและตรงกับสภาพความเป็นจริงมากที่สุด ทั้งนี้ สามารถ Download แบบสอบถาม เพื่อศึกษาและทำความเข้าใจข้อคำถามได้ที่ <http://www.etcommission.go.th> และตอบแบบสอบถามออนไลน์ได้ที่ <https://www.surveycan.com/survey119113>
3. ข้อมูลที่ได้รับนี้จะเก็บเป็นความลับ และจะนำเสนอผลการศึกษาในภาพรวมเท่านั้น
4. ถ้าต้องการทราบรายละเอียดเพิ่มเติมเกี่ยวกับการบันทึกแบบสอบถาม ติดต่อสอบถามที่สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

คุณณัฐพงษ์ พงษ์วิทยานุกฤต	โทรศัพท์ 02-1421343	อีเมล natthaphong.p@mict.go.th
คุณธีรวดี สุภาวนิตย์	โทรศัพท์ 02-1417001	อีเมล teeravadee.s@mict.go.th
คุณปริญญา ก้อยจะบก	โทรศัพท์ 02-1416997	อีเมล parinya.k@mict.go.th

ชื่อของหน่วยงาน

- () องค์การบริหารส่วนจังหวัด ระบุชื่อ.....
- () เทศบาลนคร ระบุชื่อ.....
- () เทศบาลเมือง ระบุชื่อ.....
- () เทศบาลตำบล ระบุชื่อ.....
- () องค์การบริหารส่วนตำบล ระบุชื่อ.....

ส่วนที่ 1 ข้อมูลทั่วไปเกี่ยวกับระบบสารสนเทศขององค์กรปกครองส่วนท้องถิ่น

1. กรรรมสิทธิ์ของสินทรัพย์ระบบสารสนเทศของหน่วยงานมีลักษณะอย่างไร
 - () ทรัพย์สินสารสนเทศเป็นของหน่วยงานทั้งหมด
 - () ทรัพย์สินสารสนเทศเป็นการเช่าเอกชนทั้งหมด
 - () ทรัพย์สินสารสนเทศเป็นของหน่วยงานบางส่วน และเป็นการเช่าเอกชนบางส่วน
 - () อื่น ๆ โปรดระบุ

2. หน่วยงานของท่านมีการบริหารจัดการระบบสารสนเทศของหน่วยงานอย่างไร
 - () เจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่นดำเนินการเองทั้งหมด
 - () จ้างเอกชนดำเนินการทั้งหมด
 - () เจ้าหน้าที่องค์กรปกครองส่วนท้องถิ่นดำเนินการเองบางส่วน และจ้างเอกชนดำเนินการบางส่วน
 - () อื่น ๆ โปรดระบุ.....
3. หน่วยงานของท่านมีการอนุญาตให้บุคคลภายนอกใช้งานระบบสารสนเทศ หรือไม่
 - () มี
 - () ไม่มี
4. หน่วยงานของท่านมีอุปกรณ์คอมพิวเตอร์ ชนิดใดบ้าง (เลือกได้มากกว่า 1 ข้อ)
 - () เครื่องคอมพิวเตอร์แม่ข่าย
 - () เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ
 - () เครื่องคอมพิวเตอร์แบบพกพา
 - () แท็บเล็ต
 - () สมาร์ทโฟน
 - () อื่น ๆ โปรดระบุ
5. หน่วยงานของท่านมีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ที่นำมาใช้ปฏิบัติงานในหน่วยงาน หรือไม่
 - () มี
 - () ไม่มี
6. หน่วยงานของท่านมีการอนุญาตให้ผู้บริหารและเจ้าหน้าที่นำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้ภายในหน่วยงาน หรือไม่
 - () มี
 - () ไม่มี
7. หน่วยงานของท่านมีการเชื่อมต่อระบบเครือข่ายแบบใด
 - () มีสาย
 - () ไร้สาย
 - () ทั้งสองแบบ
8. หน่วยงานของท่านมีการเชื่อมต่อระบบเครือข่ายกับผู้ให้บริการรายใด
 - () เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (Government Information Network หรือ GIN)
 - () บริษัท ทีโอที จำกัด (มหาชน) (โดยไม่ผ่านเครือข่าย GIN)
 - () บริษัท กสท โทรคมนาคม จำกัด (มหาชน) (โดยไม่ผ่านเครือข่าย GIN)
 - () ผู้ให้บริการรายอื่น โปรดระบุ

9. หน่วยงานของท่านมีการใช้จ่ายงบประมาณด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อปีงบประมาณเท่าใด
- () ไม่เกิน 5 ล้านบาท
 - () ตั้งแต่ 5 ล้านบาทขึ้นไป แต่ไม่เกิน 50 ล้านบาท
 - () ตั้งแต่ 50 ล้านบาทขึ้นไป แต่ไม่เกิน 100 ล้านบาท
 - () ตั้งแต่ 100 ล้านบาทขึ้นไป
10. หน่วยงานของท่านมีการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-Mail) หลักจากที่ได้
- () ใช้บริการจากจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ (Mail.go.th)
 - () ใช้บริการของหน่วยงานตนเอง
 - () ใช้บริการจากหน่วยงานรัฐอื่น (เช่น กรมส่งเสริมการปกครองส่วนท้องถิ่น เป็นต้น)
 - () ใช้บริการจากบริการ e-Mail ฟรี (เช่น gmail.com, hotmail.com , yahoo.com เป็นต้น)
 - () อื่น ๆ โปรดระบุ
11. หน่วยงานของท่านมีเว็บไซต์เพื่อเผยแพร่ข้อมูลข่าวสารให้กับประชาชน หรือไม่
- () มี
 - () ไม่มี
12. หน่วยงานของท่านมีการพัฒนาระบบสารสนเทศขึ้นมาใช้งานเอง หรือไม่
- () มี ระบุ
 - () ไม่มี
13. หน่วยงานของท่านมีการใช้งานระบบสารสนเทศที่พัฒนาหรือจัดทำโดยกรมส่งเสริมการปกครองส่วนท้องถิ่น หรือไม่
- () มี ระบุ
 - () ไม่มี
14. หน่วยงานของท่านมีการใช้งานระบบสารสนเทศที่พัฒนาหรือจัดทำโดยหน่วยงานรัฐอื่นที่นอกเหนือจากกรมส่งเสริมการปกครองส่วนท้องถิ่น หรือไม่
- () มี ระบุ
 - () ไม่มี
15. หน่วยงานของท่านมีการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลของประชาชนและเจ้าหน้าที่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ สำหรับใช้ในการปฏิบัติงาน หรือไม่
- () มี
 - () ไม่มี

16. ระบบสารสนเทศของหน่วยงานท่านเคยถูกโจมตีจากภายนอก เช่น หน้าจอของเว็บไซต์ถูกเปลี่ยนแปลงโดยผู้ที่ไม่ได้รับอนุญาต หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
17. ระบบสารสนเทศของหน่วยงานท่านมีการถูกโจมตีจากไวรัสคอมพิวเตอร์ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ

ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

โปรดทำเครื่องหมาย ✓ ในช่อง () ที่หน่วยงานของท่านดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

1.1 มีการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

1.2 มีการประกาศหรือแจ้งนโยบายดังกล่าวให้เจ้าหน้าที่ทั้งภายในและภายนอกหน่วยงานรับทราบหรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1 ผู้บริหารมีการสนับสนุนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศหรือไม่ (เช่น งบประมาณ บุคลากร อุปกรณ์ เป็นต้น)

- () มี
- () ไม่มี
- () ไม่แน่ใจ

2.2 ผู้บริหารมีการมอบหมายภารกิจด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้กับเจ้าหน้าที่อย่างชัดเจนหรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

2.3 มีการกำหนดขั้นตอนการพัฒนาระบบสารสนเทศใหม่ ให้สามารถทำงานร่วมกับระบบสารสนเทศเดิมได้หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

2.4 มีการจัดทำบันทึกข้อตกลงให้เจ้าหน้าที่ต้องรักษาข้อมูลที่เป็นความลับ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

2.5 มีการจัดทำข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในกรณีที่อนุญาตให้บุคคลหรือหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

3. การบริหารจัดการทรัพย์สินสารสนเทศ

3.1 มีการเก็บบันทึกและจำแนกประเภทของข้อมูลสารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศหรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

4.1 มีการกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

4.2 มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างจะต้องปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

4.3 มีการกำหนดบทลงโทษ ในกรณีที่เจ้าหน้าที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

- 4.4 มีการกำหนดหน้าที่ความรับผิดชอบของผู้รับจ้างในกรณีที่มีการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้าง หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 4.5 มีการกำหนดให้เจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงาน เมื่อสิ้นสุดการจ้างงาน หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 4.6 มีการกำหนดให้ยกเลิกสิทธิของเจ้าหน้าที่หรือบุคคลภายนอกที่หน่วยงานว่าจ้าง ในการเข้าใช้งานระบบสารสนเทศ เมื่อสิ้นสุดการจ้างงาน หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 4.7 มีการปรับเปลี่ยนสิทธิในการใช้งานระบบสารสนเทศ เมื่อเจ้าหน้าที่มีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ

5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

- 5.1 มีการกำหนดพื้นที่ติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศ เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์คอมพิวเตอร์ หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 5.2 มีการป้องกันภัยคุกคามต่างๆ ที่อาจเกิดขึ้น (เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น) เพื่อป้องกันไม่ให้อุปกรณ์สารสนเทศเสียหาย หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ

- 5.3 มีการจัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรือเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 5.4 มีการจัดเตรียมอุปกรณ์ป้องกัน (เช่น เครื่องสำรองไฟ เครื่องปั่นไฟ เป็นต้น) เพื่อป้องกันการล้มเหลวของระบบต่างๆ (เช่น ระบบกระแสไฟฟ้า ระบบปรับอากาศ เป็นต้น) หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 5.5 มีการบำรุงรักษาและดูแลอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ**
- 6.1 มีการจัดทำและปรับปรุงคู่มือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบต่าง ๆ เพื่อให้เจ้าหน้าที่สามารถนำไปปฏิบัติได้อย่างถูกต้องและปลอดภัย หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 6.2 มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงาน ต้องปฏิบัติตามสัญญาหรือข้อตกลงในการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ
- 6.3 มีการติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอก หรือไม่
- () มี
- () ไม่มี
- () ไม่แน่ใจ

- 6.4 มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการพัฒนาหรือปรับปรุง หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 6.5 มีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับมาใช้ งาน หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 6.6 มีการกำหนดขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกู้คืนในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ รวมทั้งมีการสร้างความตระหนักให้กับผู้ใช้งานระบบสารสนเทศ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 6.7 มีการสำรองและทดสอบข้อมูลสารสนเทศที่สำรองเก็บไว้อย่างสม่ำเสมอ และเป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 6.8 มีการบริหารจัดการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 6.9 มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการ ในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยังผู้ให้บริการภายนอก หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ

- 6.10 มีนโยบายและขั้นตอนการปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทาง การสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ
- 6.11 มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์กับบุคคลหรือหน่วยงานภายนอก หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ
- 6.12 มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันไม่ให้ข้อมูลสารสนเทศเกิดความเสียหายในระหว่าง ที่มีการแลกเปลี่ยนข้อมูลของระบบสารสนเทศ หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ
- 6.13 มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (เช่น การสั่งซื้อ/ขายสินค้าหรือบริการผ่านระบบอิเล็กทรอนิกส์ การชำระเงินผ่านระบบ อิเล็กทรอนิกส์ เป็นต้น) หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ
- 6.14 มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (เช่น การยื่นชำระค่าธรรมเนียมผ่านทางอินเทอร์เน็ต การทำสัญญาทางอิเล็กทรอนิกส์ทางอินเทอร์เน็ต เป็นต้น) หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ
- 6.15 มีการตรวจสอบความครบถ้วนและถูกต้องของข้อมูลสารสนเทศที่มีการเผยแพร่สู่สาธารณะ และ ป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือไม่
- มี
- ไม่มี
- ไม่แน่ใจ

6.16 มีการเก็บบันทึกและตรวจสอบข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

6.17 หน่วยงานของท่านมีการเฝ้าระวัง ติดตาม สังเกตการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

6.18 มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไข เปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

6.19 มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศของผู้ดูแลระบบ หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

7.1 มีการกำหนดนโยบายควบคุมการเข้าถึงระบบเป็นลายลักษณ์อักษร และมีการปรับปรุงตามระยะเวลาที่กำหนด หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

7.2 มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการ หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

- 7.3 มีการกำหนดสิทธิในการเข้าใช้งานระบบสารสนเทศ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 7.4 มีการกำหนดให้ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มีการใช้งาน หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 7.5 มีการควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 7.6 มีการกำหนดให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการ ตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 7.7 มีการกำหนดให้ผู้ใช้งานระบุตัวตนในการเข้าใช้งานระบบ เช่น Username Password เพื่อพิสูจน์ตัวตนก่อนเข้าใช้งานระบบสารสนเทศ หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ
- 7.8 มีการกำหนดให้ระบบมีการตัดและหมดเวลาการใช้งาน หลังจากที่ไม่มีการใช้งานภายในระยะเวลาที่กำหนด หรือไม่
- () มี
 - () ไม่มี
 - () ไม่แน่ใจ

7.9 มีการกำหนดให้ระบบมีการพักหรือล้างหน้าจอ หลังจากที่ไม่มีการใช้งานภายในระยะเวลาที่กำหนดหรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

7.10 มีการจำกัดการเข้าถึงและใช้งานระบบสารสนเทศ โดยให้ผู้ใช้งานเข้าถึงเฉพาะข้อมูลสารสนเทศและฟังก์ชันตามที่หน่วยงานกำหนด หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

7.11 มีการกำหนดนโยบายและข้อปฏิบัติในการใช้คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หรือไม่ (เช่น เครื่องคอมพิวเตอร์แบบพกพา, สมาร์ทโฟน เป็นต้น) หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

8.1 มีการจัดทำข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไว้ในเงื่อนไขการจ้างพัฒนาหรือปรับปรุงระบบ หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

8.2 มีการดูแล ควบคุม ติดตามตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก รวมถึงการจ้างช่วงพัฒนาซอฟต์แวร์ด้วย หรือไม่

- มี
- ไม่มี
- ไม่แน่ใจ

9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

9.1 มีการรายงานสถานการณ์ด้านการรักษาความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดให้ผู้บังคับบัญชาทราบโดยเร็ว หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

10. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1 หน่วยงานของท่านมีการจัดทำแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศหลังเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานภายในระยะเวลาที่กำหนดไว้ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

11.1 มีการกำหนดแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมาย ระเบียบของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

11.2 มีการป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

11.3 มีการกำหนดให้เจ้าหน้าที่ของหน่วยงานต้องดูแลรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้สอดคล้องกับกฎ ระเบียบของหน่วยงาน หรือไม่

- () มี
- () ไม่มี
- () ไม่แน่ใจ

ส่วนที่ 3 การพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. เจ้าหน้าที่ของหน่วยงานที่ดูแลระบบสารสนเทศส่วนใหญ่มีวุฒิการศึกษาในสาขาใด
() สาขาคอมพิวเตอร์หรือสาขาเทคโนโลยีสารสนเทศ
() สาขาอื่น ๆ ระบุ.....
2. เจ้าหน้าที่ของหน่วยงานที่ดูแลระบบสารสนเทศมีการเพิ่มพูนทักษะและความสามารถโดยวิธีการใด (เลือกได้มากกว่า 1 ข้อ)
() ศึกษาต่อเนื่องในระดับที่สูงขึ้น เพื่อให้ได้วุฒิการศึกษาเพิ่มเติม
() ฝึกอบรมหลักสูตรระยะสั้นหรือระยะกลางเพิ่มเติม
() เรียนรู้ด้วยตนเองจากหนังสือหรืออินเทอร์เน็ต
() ศึกษาดูงานจากหน่วยงานอื่น
() อื่น ๆ ระบุ.....
3. เจ้าหน้าที่ของหน่วยงานที่ดูแลระบบสารสนเทศควรได้รับการเพิ่มพูนองค์ความรู้และทักษะในเรื่องใดบ้าง (เลือกได้มากกว่า 1 ข้อ)
() แนวโน้มเทคโนโลยีสารสนเทศในอนาคต
() แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ
() การป้องกันไวรัส
() การป้องกันการเจาะระบบ
() การกู้คืนระบบ
() กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
() กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
() การใช้งานอุปกรณ์คอมพิวเตอร์
() การใช้งานโปรแกรมประยุกต์
() มาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
() การบริหารจัดการระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
() อื่น ๆ ระบุ

ส่วนที่ 4 ข้อเสนอแนะที่ต้องการได้รับการสนับสนุนจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

1.
.....
.....
2.
.....
.....
3.
.....
.....
4.
.....
.....
5.
.....
.....

ขอขอบคุณยิ่ง