นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมตรวจบัญชีสหกรณ์

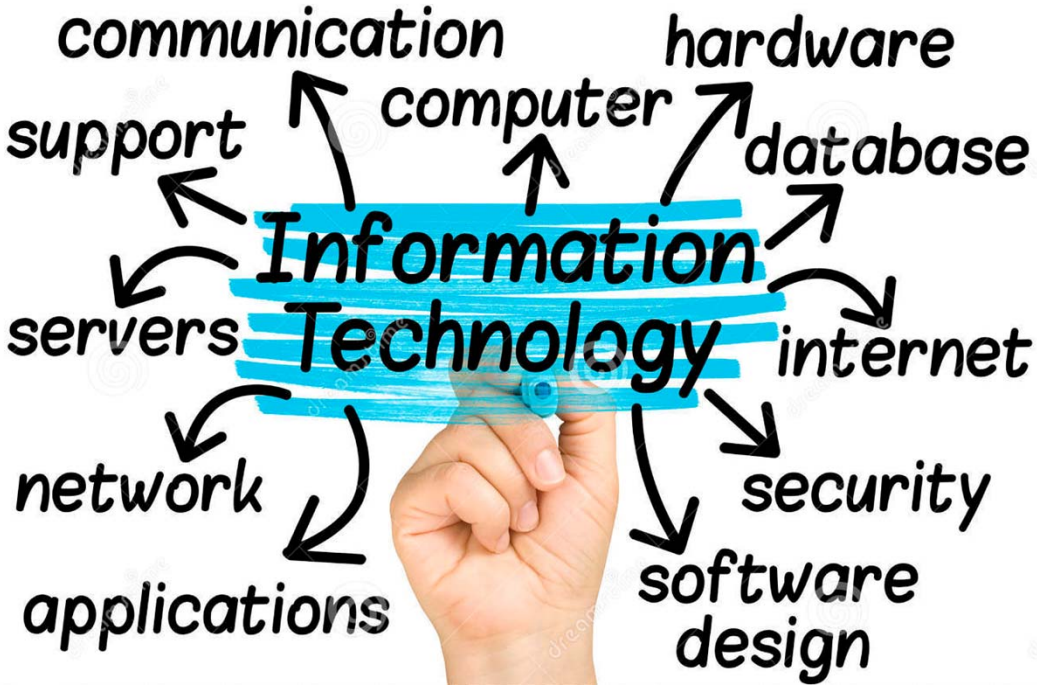
www.cad.go.th

ผู้บรรยาย : นางสาวกนกพรรณ ชำนาญกิจ
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

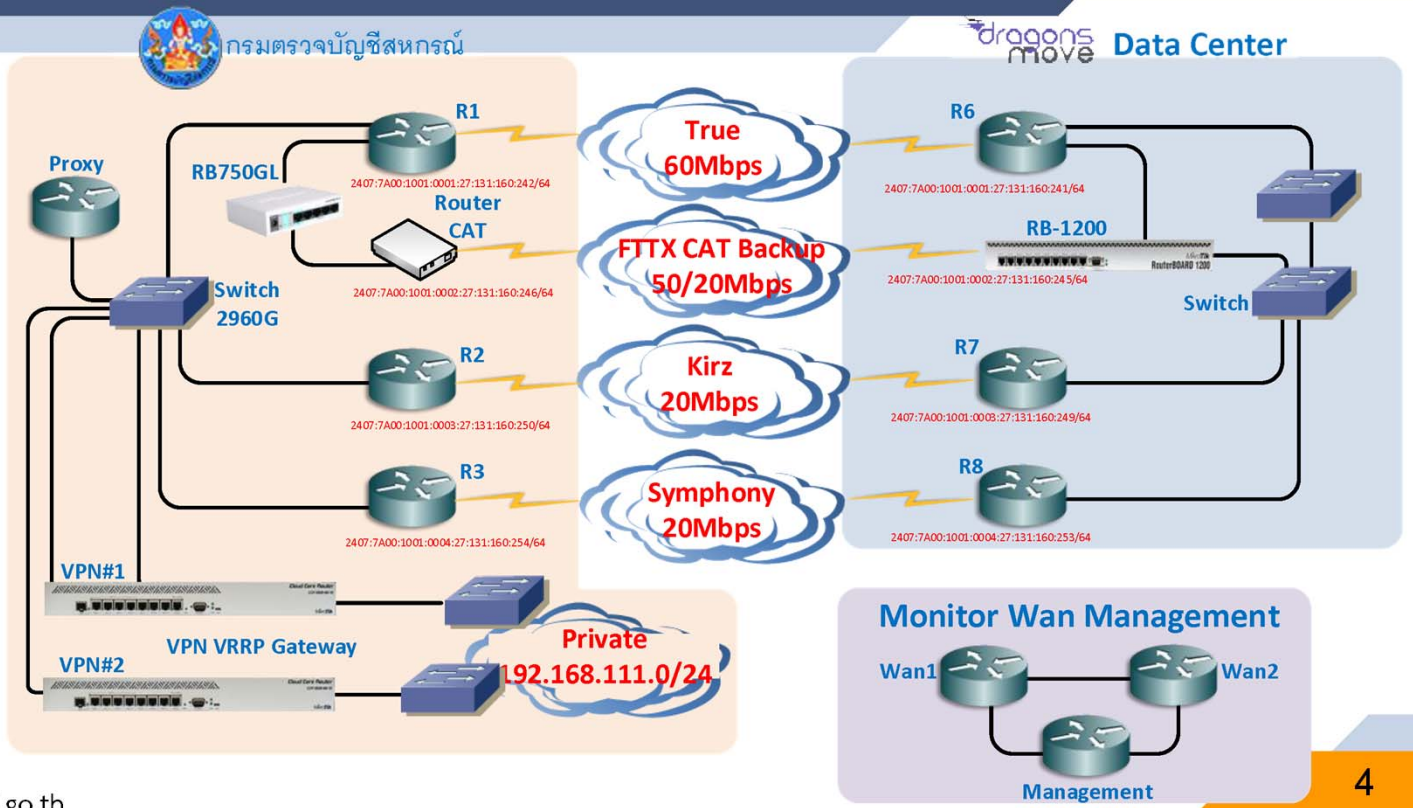
หัวข้อการในการบรรยาย

- ระบบสารสนเทศและระบบเครือข่ายของกรมตรวจบัญชีสหกรณ์
- ทำไมต้องมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ?
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมตรวจบัญชีสหกรณ์

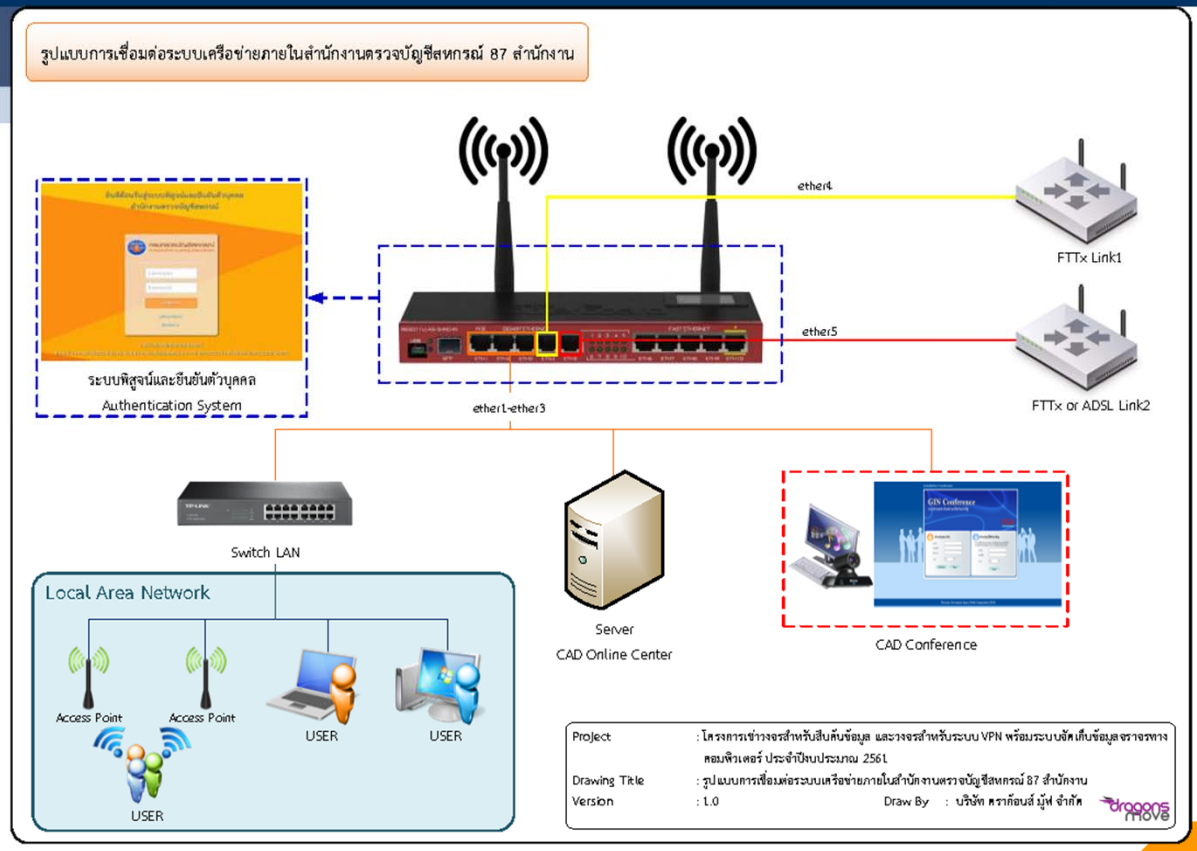
ระบบเทคโนโลยีสารสนเทศ



ระบบเครือข่ายของกรมตรวจบัญชีสหกรณ์



ระบบเครือข่ายของสำนักงานตรวจบัญชีสหกรณ์



www.cad.go.th

ทำไมต้องมีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 และมาตรา 7 **กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

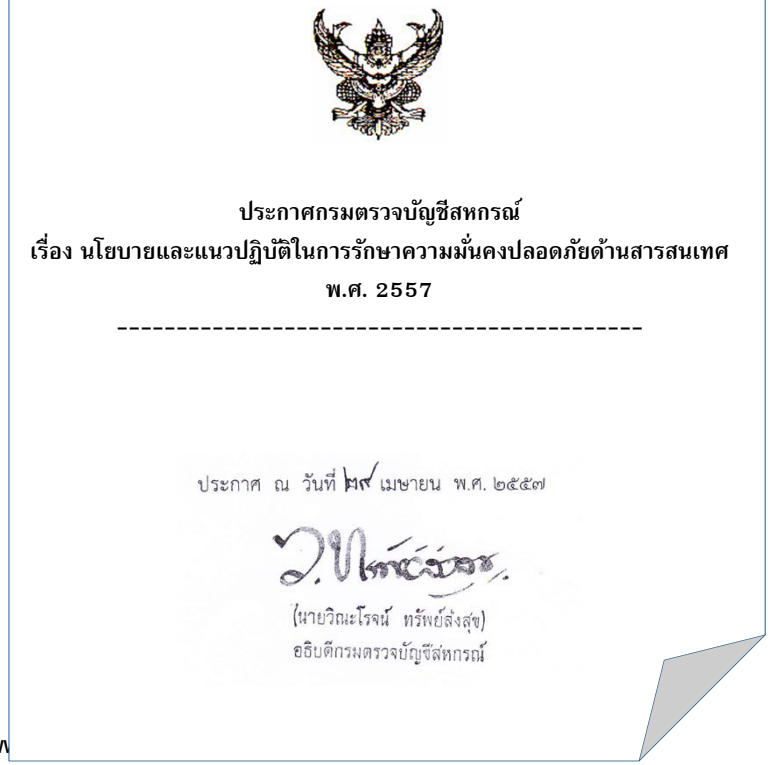
(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

ประกาศสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร



ประกาศกรมตรวจบัญชีสหกรณ์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. 2557

ประกาศ ณ วันที่ ๒๙ เมษายน พ.ศ. ๒๕๕๗

(นายวิณะโรจน์ ทรัพย์สังสุข)
อธิบดีกรมตรวจบัญชีสหกรณ์

ประกาศสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง รายชื่อหน่วยงานที่ผ่านความเห็นชอบตามมาตรา 7 ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ว่าด้วยการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2557

www

ขอความร่วมมือหน่วยงานของรัฐในการดำเนินงานภายใต้พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549

หน่วยงาน	การดำเนินงาน
1. หน่วยงานของรัฐที่ยังไม่ได้ดำเนินการเพื่อให้เป็นไปตามภายใต้พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 มาตรา 6 และมาตรา 7	ขอให้ดำเนินการจัดทำ 1. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ 2. นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)
2. หน่วยงานของรัฐที่ได้เคยจัดส่งแบบประเมินประกอบการพิจารณาการดำเนินงานตามนโยบายและแนวปฏิบัติ ภายใต้มาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์ภาครัฐ พ.ศ. 2549 และได้รับการประสานงานเพื่อปรับแก้ไข จำนวน 72 หน่วยงาน	ขอให้เร่งรัดการปรับแก้ไขรายละเอียดนโยบายและแนวปฏิบัติฯ ให้มีความครบถ้วนตามที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดและนำเสนอคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อขอความเห็นชอบ ตามมาตรา 7
3. หน่วยงานที่เคยได้รับการเห็นชอบและประกาศรายชื่อไปแล้วเป็นเวลาอย่างน้อย 2 ปี จำนวน 40 หน่วยงาน	ขอให้ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้มีความเป็นปัจจุบัน และสอดคล้อง ครบถ้วน ตามเจตนาที่กฎหมายกำหนดไว้ และนำเสนอผลการทบทวนต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์อีกครั้ง

แจ้งผลการพิจารณานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ (ฉบับทบทวน)

หนังสือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ที่ ดศ 0207/8615 ลงวันที่ 5 ตุลาคม 2560
แจ้งให้ทราบว่าคณะกรรมการธุรกรรมทาง
อิเล็กทรอนิกส์ได้มีมติในการประชุม ครั้งที่ 5/2560
เมื่อวันที่ 25 กันยายน 2560 ให้ความเห็นชอบต่อ
นโยบายและแนวปฏิบัติในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์
(ฉบับทบทวน)

ประกาศกรมตรวจบัญชีสหกรณ์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมตรวจบัญชีสหกรณ์ พ.ศ. 2560

ประกาศ ณ วันที่ ๑๖ ตุลาคม พ.ศ. ๒๕๖๐

(นายโอภาส หองยงค์)
อธิบดีกรมตรวจบัญชีสหกรณ์

www.cad.go.th

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์

วัตถุประสงค์

1. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหารระดับสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บังคับบัญชา ผู้ดูแลระบบ และผู้ใช้งานของ กตส. ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ของ กตส. ดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล

3. เพื่อเผยแพร่ให้ผู้บริหารระดับสูงสุด ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บังคับบัญชา ผู้ดูแลระบบ และผู้ใช้งานของ กตส. ได้รับทราบ และต้องถือปฏิบัติตามนโยบายอย่างเคร่งครัด

ขอบเขตการดำเนินงาน

1. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ
    - 1.1 การควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย
    - 1.2 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ
    - 1.3 การควบคุมการเข้าถึงระบบปฏิบัติการ
    - 1.4 การควบคุมการเข้าถึงระบบเครือข่าย
2. การจัดทำระบบสำรองของระบบสารสนเทศ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

สร้างความรู้ความเข้าใจ

ผู้รับผิดชอบ

ระบบคอมพิวเตอร์
หรือ
ข้อมูลสารสนเทศ

บกพร่อง

ละเลย

ฝ่าฝืนการ
ปฏิบัติ

ศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสาร

ผู้บริหารระดับสูง
(Chief Executive Officer : CEO

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ของกรมตรวจบัญชีสหกรณ์ พ.ศ. 2560

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ แบ่งออกเป็น 7 หมวด

หมวดที่ 1. แนวปฏิบัติในการควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย

หมวดที่ 2. แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศ

หมวดที่ 3. แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

หมวดที่ 4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

หมวดที่ 5. แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

หมวดที่ 6 แนวปฏิบัติในการสำรองข้อมูล

หมวดที่ 7 แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

หมวดที่ 1. แนวปฏิบัติในการควบคุมการเข้าถึงห้องควบคุมระบบเครือข่าย

- กำหนดสิทธิบุคคล
- สแกนลายนิ้วมือ
- ลงบันทึกการเข้า-ออก
- กรณีเป็นบุคคลภายนอกต้องได้รับอนุญาต
- ต้องมีเจ้าหน้าที่อยู่ภายในห้องเมื่อมีบุคคลภายนอก

- ทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง

www.cad.go.th

หมวดที่ 2. แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และระบบสารสนเทศ

ผู้รับผิดชอบระบบสารสนเทศ

1. จัดการควบคุมการเข้าถึงระบบสารสนเทศ
2. การจัดเก็บข้อมูล
   - ประเภทของข้อมูล
   - ระดับความสำคัญของข้อมูล
3. ระบบต้องสามารถเข้าถึงได้ 24 ชั่วโมง โดยผ่านช่องทางอินเตอร์เน็ต
4. บริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน
   - 4.1 ลงทะเบียนผู้ใช้งาน
   - 4.2 กำหนดสิทธิการใช้ระบบสารสนเทศแก่บุคคลภายนอก
   - 4.3 สิทธิพิเศษกับผู้ใช้งาน
5. บริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของผู้ใช้งาน
6. ต้องมีการพิสูจน์ตัวตน
7. ต้องกำหนดการบริหารจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย (8 ตัวอักษร = ตัวเลข + ตัวอักษร)
8. จ้าง Outsource ต้องลงนามในการรักษาความลับ
9. การจัดการกับข้อมูลลับ
10. การทำลายข้อมูลอิเล็กทรอนิกส์
11. แยกระบบสารสนเทศที่ไวต่อการรบกวน
12. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
13. การปฏิบัติงานจากภายนอกสำนักงาน

กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ตามมาตรฐาน DoD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายใช้ใหม่ได้	วิธีทำลาย	ระยะเวลาทำลาย
กระดาษ	-	• ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format	• ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ • ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	• ใช้การหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน	เก็บรักษาไว้อย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด
เทป	-	• ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผา ทำลาย	เก็บรักษาไว้อย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด
ฮาร์ดดิสก์	ใช้วิธีการ Format	• ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ • ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด

หมวดที่ 3. แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

ผู้ใช้งาน

- ต้องยืนยันตัวตนก่อนเข้างานระบบปฏิบัติการทุกครั้ง
- ต้องไม่อนุญาตให้บุคคลอื่นใช้ username, password ของตนเอง

ผู้ดูแลระบบ

- ตั้งค่าระบบให้แจ้งเตือนเมื่อมีการใส่รหัสผิดเกิน 3 ครั้ง

- จำกัดการใช้งานทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งาน

www.cad.go.th

หมวดที่ 4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

ผู้ดูแลระบบ

1. ต้องแบ่งโซนกลุ่มเครือข่าย

2. จำกัดสิทธิการใช้งานเฉพาะเครือข่ายที่อนุญาตเท่านั้น

6. ทบทวนบัญชีและสิทธิผู้ใช้งานอย่างสม่ำเสมอ

7. IP Address ต้องมีการป้องกันมิให้หน่วยงานภายนอกเห็น

8. ห้ามต่ออุปกรณ์เครือข่ายส่วนกลาง Router, Switch, WIFI ก่อนได้รับอนุญาต

16. เก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ IP Address และสถานที่ตั้ง

12. มีสิทธิระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานผิดนโยบาย

14. ต้องมีการเก็บ Log 90 วัน

17. ทำการตรวจสอบอุปกรณ์เครือข่ายโดยใช้ MAC Address, IP Address เพื่อเป็นการยืนยัน

18. เปิดพอร์ตต่อเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป นอกเหนือที่กำหนดต้องได้รับการยินยอมจาก ศทส.

15. จัดทำผังระบบเครือข่าย Network Diagram

13. ตรวจสอบเหตุการณ์ข้อมูลจราจร พฤติกรรมการใช้งาน หากเกิดเหตุที่มีความเสี่ยงต้องรายงานผู้บังคับบัญชา

19. กำหนดการเปิด-ปิดพอร์ตของอุปกรณ์เครือข่าย โดยปิดพอร์ตที่มีความเสี่ยง

20. ยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่จำเป็นใช้งาน

21. แยกเครือข่ายเป็นย่อย ๆ ตามอาคารต่าง ๆ

24. Gateway เพื่อควบคุมการเข้าถึงเครือข่ายทั้งภายในและภายนอกหน่วยงาน

23. ต้องใช้ Firewall กั้น หรือแบ่งเครือข่ายภายในออกเป็นย่อย ๆ

26. จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย

22. แบ่งเครือข่ายภายในหน่วยงานออกเป็น ภายใน, ภายนอก

25. ต้องตรวจสอบ Gateway หรืออุปกรณ์เครือข่าย IP Address เพื่อควบคุมการไหลของข้อมูล

27. ตรวจสอบและกำหนดเส้นทางบนเครือข่ายให้เหมาะสมให้เป็นไปตามนโยบายควบคุมการเข้าถึงของหน่วยงาน

หมวดที่ 4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (ต่อ)

บุคคลภายนอก

9. ต้องขออนุญาตในการใช้งานระบบเครือข่าย

ผู้ใช้งาน

3. ต้องไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายจากบัญชีของตนเอง

4. การ Remote Access VPN ผู้ใช้งานต้องมีการพิสูจน์ตัวตน Authentication

5. การเข้าสู่ระบบ Internet ต้องลงบันทึก Login & Authentication

10. ห้ามดาวน์โหลดไฟล์หรืออัพโหลดไฟล์ขนาดใหญ่เกินไป หรือดูหนังฟังเพลงในระหว่างเวลาปฏิบัติงาน

11. การนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายของหน่วยงานต้องได้รับอนุญาต

การควบคุมการเข้าใช้งานระบบจากภายนอก

1. การ Remote Access มีช่องโหว่ ต้องมีการควบคุมการเข้าสู่ระบบ

2. ผู้ใช้งาน ต้องทำหนังสือระบุเหตุผลหรือความจำเป็นในการเข้าสู่ระบบจากระยะไกล

3. ผู้ดูแลระบบต้องไม่เปิดพอร์ตในการเข้าสู่ระบบข้อมูลจากระยะไกล Remote Access ทิ้งไว้โดยไม่จำเป็น

หมวดที่ 5. แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

หน้าที่และความรับผิดชอบของผู้ใช้งาน

การควบคุมสินทรัพย์และการใช้งานระบบคอมพิวเตอร์

หมวดที่ 6 แนวปฏิบัติในการสำรองข้อมูล

ผู้ดูแลระบบ

การสำรองข้อมูล

1. Full System, Full Data Backup และ Incremental Backup
2. กำหนดวันที่ เวลาที่สำรอง ผู้รับผิดชอบ
3. ตรวจสอบความถูกต้องของการ Backup
4. บันทึกการสำรองข้อมูล Operator Logs (เริ่มต้น สิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูล รายงานให้ ผอ. ศทส.
5. รายงานข้อผิดพลาด (Fault Logging) และวิธีการแก้ไข
6. พบปัญหาการสำรองข้อมูลไม่สามารถสำรองข้อมูลได้สมบูรณ์ ให้สรุปและรายงานผลต่อ ผอ. ศทส.
7. จัดเก็บข้อมูลสำรองแยกสถานที่ต่างหาก
8. ต้องเคร่งครัดต่อกระบวนการสำรองข้อมูล
9. ทบทวนข้อมูลการสำรองอย่างน้อยทุก 6 เดือน
10. ทดสอบข้อมูลระบบสารสนเทศที่สำรองอย่างน้อยปีละ 1 ครั้ง

การกู้คืนระบบ

1. กรณีต้องกู้คืนระบบให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข และรายงานผลให้ ผอ.ศทส. ทราบ
2. ถ้าส่งผลกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งแจ้งความคืบหน้าในการกู้คืนเป็นระยะ

หมวดที่ 7 แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยง

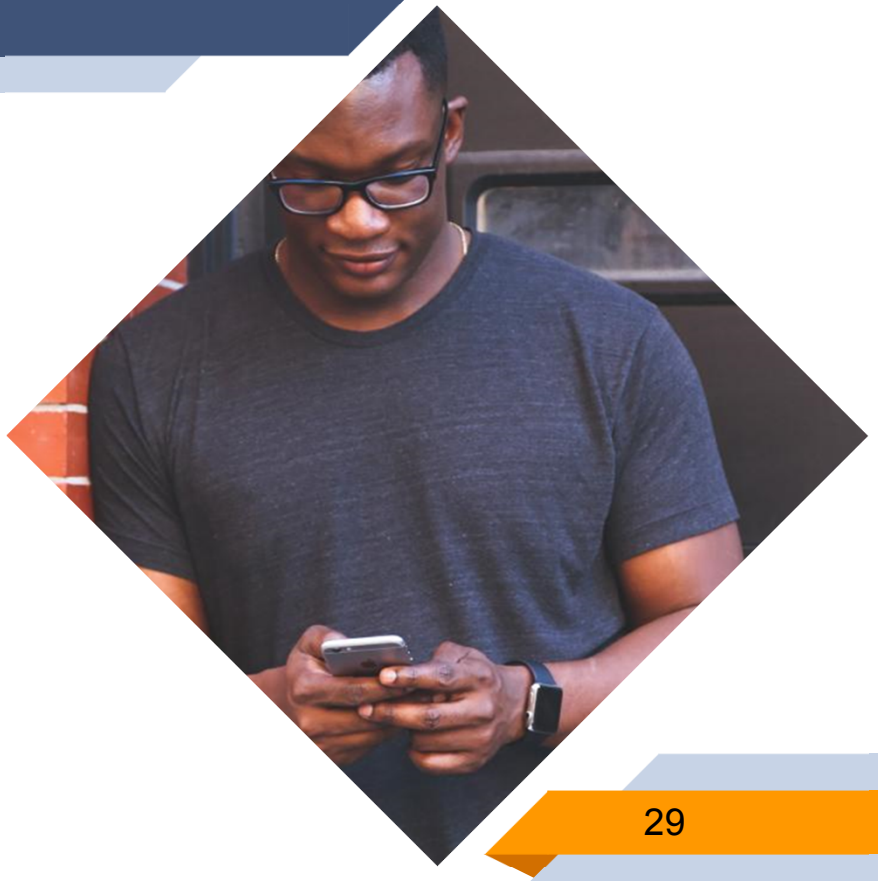
1. กระบวนการในการบริหารจัดการกับความเสี่ยงของระบบฐานข้อมูลสารสนเทศให้ปฏิบัติตามวงจรบริหารงานคุณภาพ PDCA (Plan-Do-Check-Act) Plan (วางแผน), Do (ปฏิบัติ), Check (ตรวจสอบ) และ Act (การดำเนินการให้เหมาะสม)

2. การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ

3. ต้องมีการทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง

4. ต้องมีการตรวจสอบและประเมินความเสี่ยง โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

คำถาม – คำตอบ



เอกสารสามารถ Download ได้ที่เว็บไซต์

กลุ่มระบบเครือข่ายคอมพิวเตอร์

http://netgrp.cad.go.th