

ระบบที่รองรับ มาตรฐานการรักษาความมั่นคงปลอดภัย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย

พ.ศ. ๒๕๕๕

โดยที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ กำหนดให้คณะกรรมการประกาศกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่คณะกรรมการกำหนดเป็นวิธีการที่เชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ดังต่อไปนี้

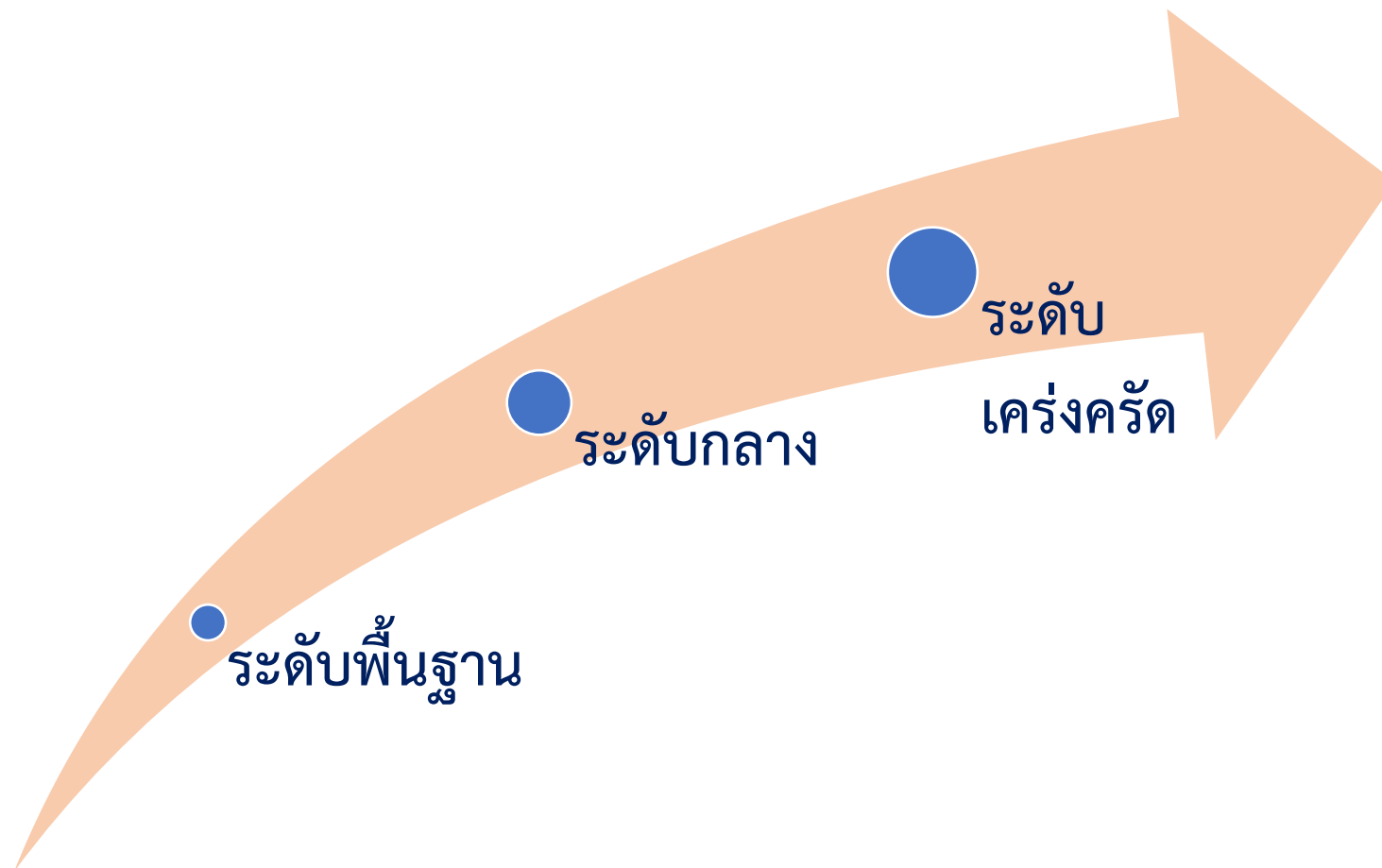
ทำยนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น ๑๑ ข้อ ได้แก่

๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
๓. การบริหารจัดการทรัพยากรสารสนเทศ
๔. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
๕. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
๖. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๗. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
๘. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
๙. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
๑๐. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง
๑๑. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

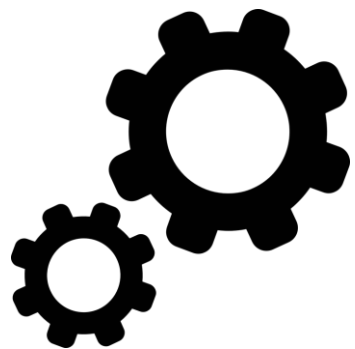
รายละเอียดสำคัญ ของ ISO27000:2005 (Annex A)

1. Security policy (5)
2. Organization of information security (6)
3. Asset management(7)
4. Human resources security (8)
5. Physical and environmental security (9)
6. Communications and operations management (10)
7. Access control (11)
8. Information systems acquisition, development and maintenance (12)
9. Information security incident management (13)
10. Business continuity management (14)
11. Compliance (15)

ระดับการรักษาความปลอดภัย

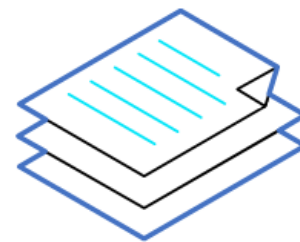


การดำเนินการตามมาตรฐาน



Process

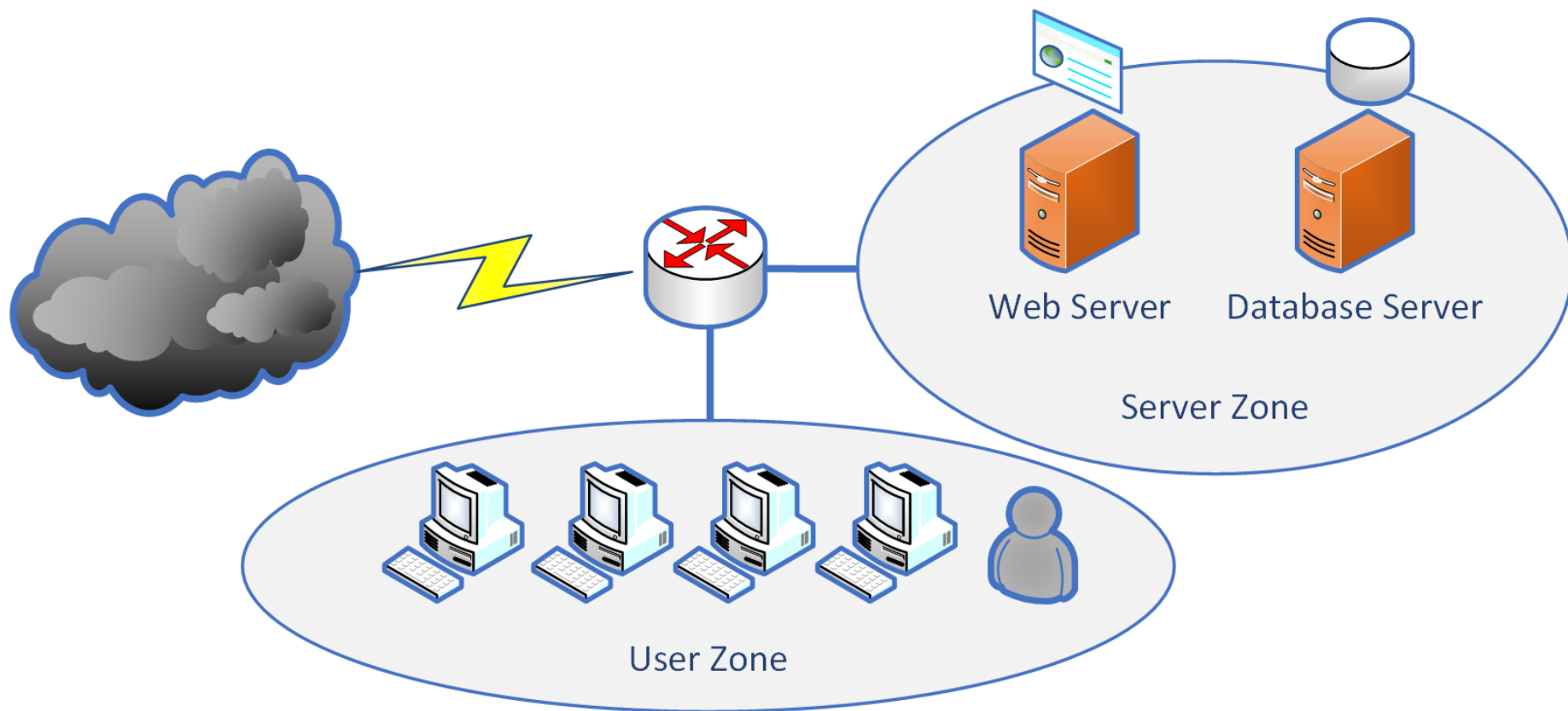
Documents



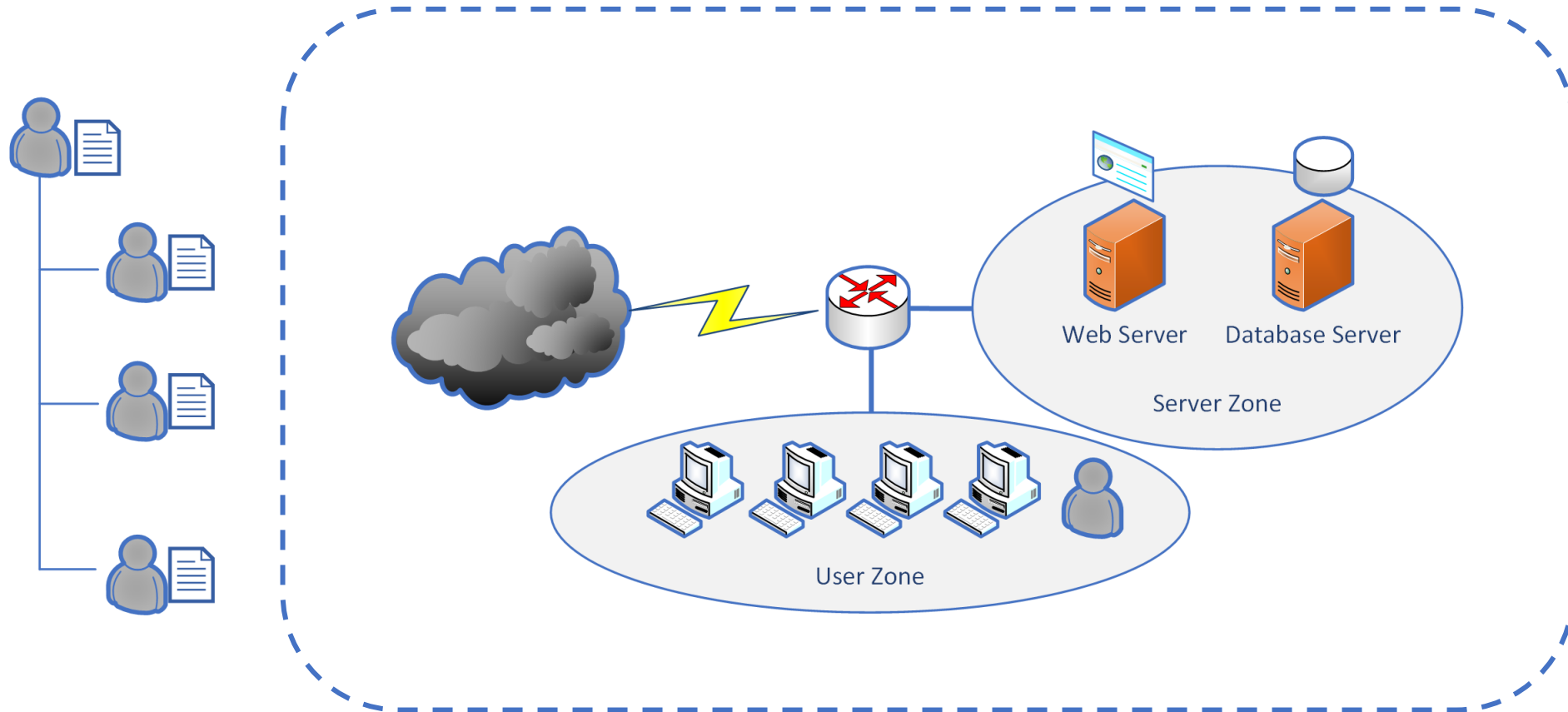
Infrastructure



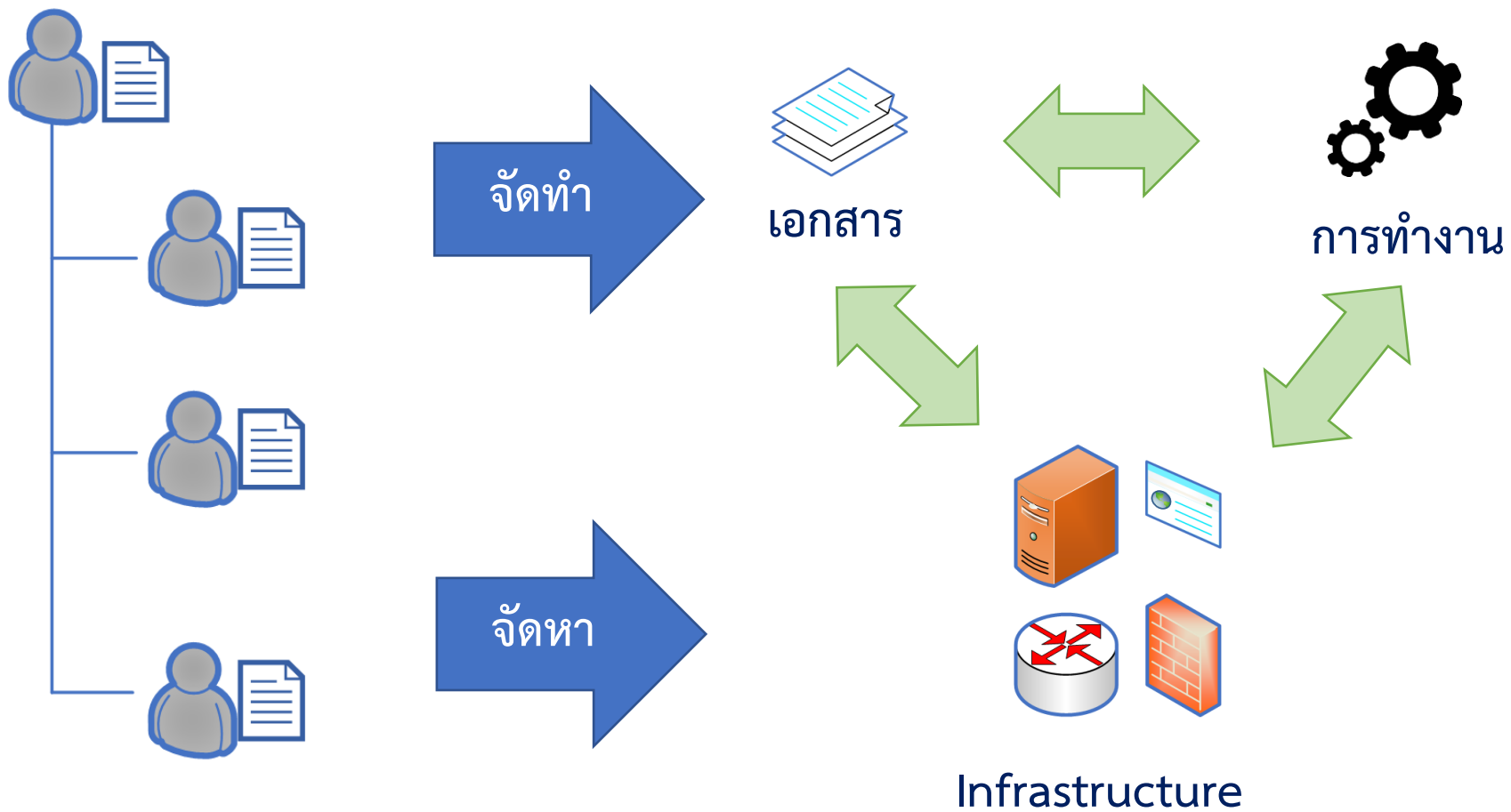
ระบบสารสนเทศตัวอย่าง

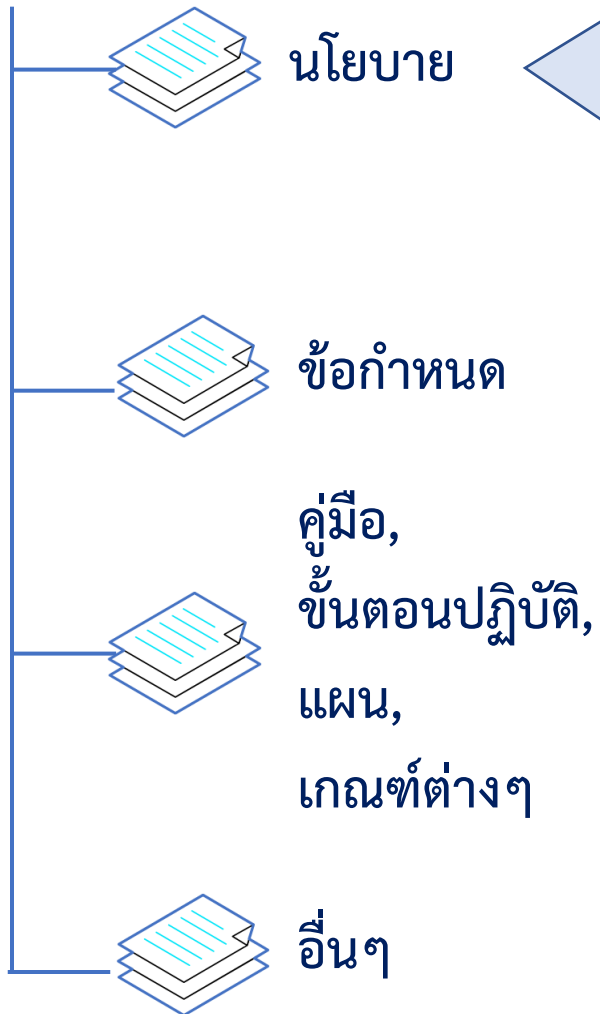


มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบ
สารสนเทศตามวิธีการแบบปลอดภัยใน
ระดับพื้นฐาน



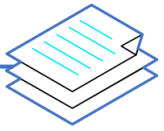
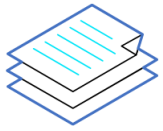
- กำหนดโครงสร้างผู้รับผิดชอบด้านการรักษาความปลอดภัย
- รายละเอียดการทำงานและความรับผิดชอบ



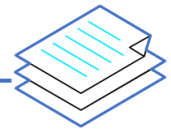


1. นโยบายการรักษาความมั่นคงปลอดภัย

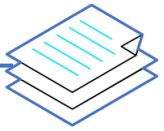
- นโยบายการเข้าถึงข้อมูลและระบบสารสนเทศ
- ลดความเสี่ยงในการใช้อุปกรณ์ที่เคลื่อนย้ายได้
- นโยบายการสำรองข้อมูล
- นโยบายในการแลกเปลี่ยนข้อมูลสารสนเทศ
- สอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน
- ป้องกันไม่ให้เกิดการใช้งานระบบสารสนเทศผิดวัตถุประสงค์



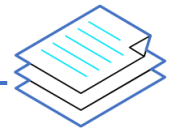
นโยบาย



ข้อกำหนด

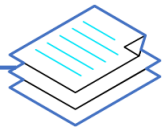


คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

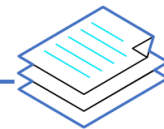


อื่นๆ

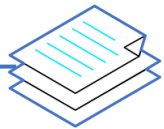
1. ข้อกำหนดในการรักษาความมั่นคงปลอดภัย (สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัย)
 - Access Control ควบคุมบุคคลภายนอก (Data , System)
2. ข้อกำหนดหน้าที่ความรับผิดชอบ: พนักงาน,หน่วยงาน,บุคคลภายนอก
 - บทลงโทษ
 - กรณียุติการจ้าง (พนักงาน,outsource) : คืนสินทรัพย์ , ยกเลิกสิทธิ
3. ข้อกำหนดในการบริหารจัดการเครือข่าย (ของหน่วยงาน , outsource)
 - Service Level Agreement
 - รูปแบบการรักษาความมั่นคงปลอดภัย
4. ข้อกำหนดการใช้งาน application
 - ออกจากระบบเมื่อไม่ใช้งาน , ปิดหน้าจอเมื่อไม่ใช้งาน
5. ข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ / ปรับปรุงระบบสารสนเทศเดิม
 - การควบคุมความมั่นคงปลอดภัยด้านสารสนเทศ
 - กำหนดรายละเอียดเกี่ยวกับการทำ Access Control ในระบบข้อมูล



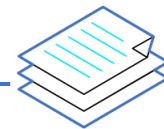
นโยบาย



ข้อกำหนด

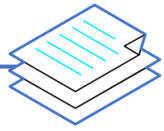
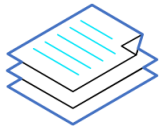


คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

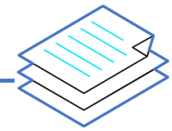


อื่นๆ

1. เอกสารขั้นตอนปฏิบัติงาน
 - การปฏิบัติงานของพนักงาน
 - การแลกเปลี่ยนข้อมูลสารสนเทศ
2. เกณฑ์การตรวจรับระบบสารสนเทศ
 - ระบบใหม่ , ปรับปรุงระบบ
 - ทดสอบในช่วงพัฒนา , ก่อนตรวจรับ
3. คู่มือการสำรองข้อมูล / การกู้คืนข้อมูล
4. Incident Response Plan
 - รายงานสถานการณ์ให้ผู้บริหาร ตามช่องทางที่เหมาะสม
ในสถานการณ์ต่างๆ
5. Business Continuity Plan



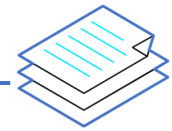
นโยบาย



ข้อกำหนด

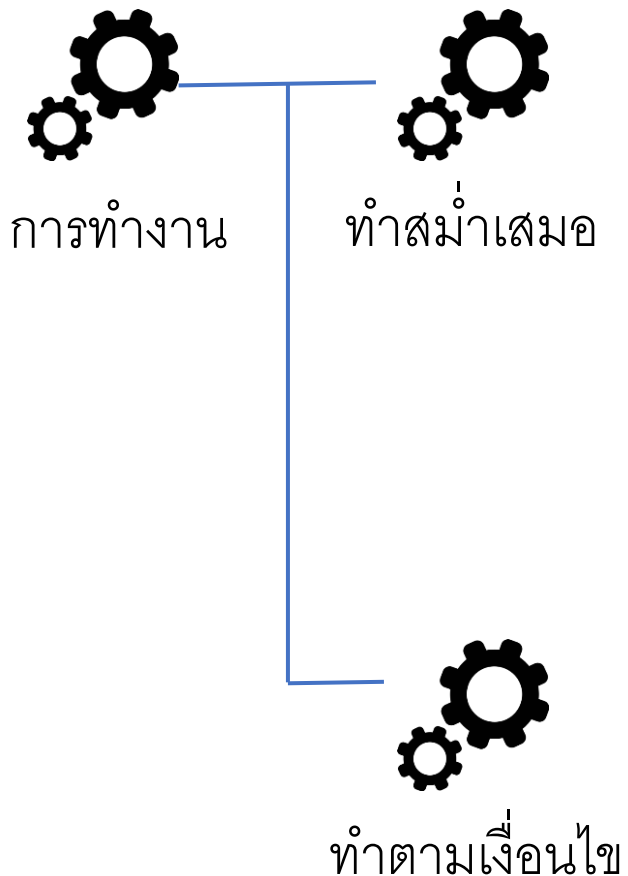


คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

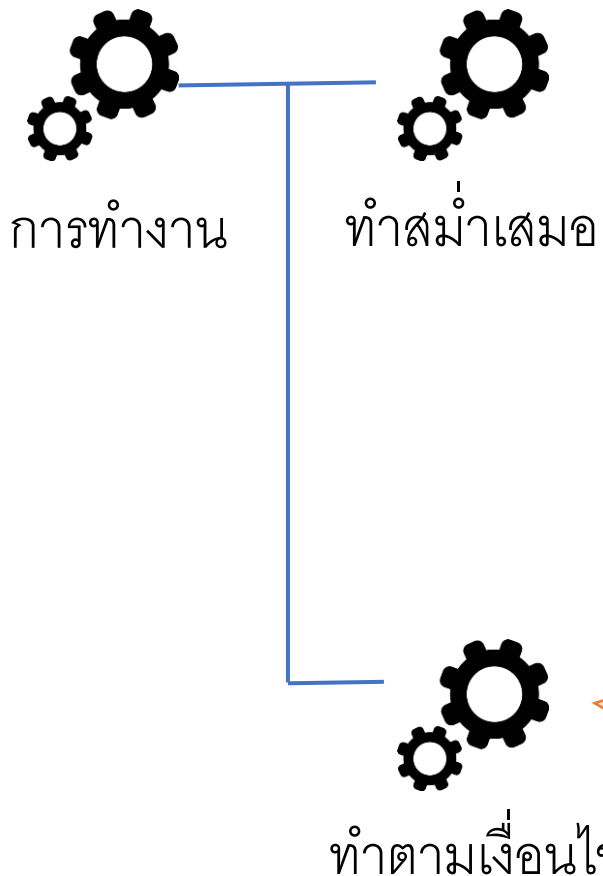


อื่นๆ

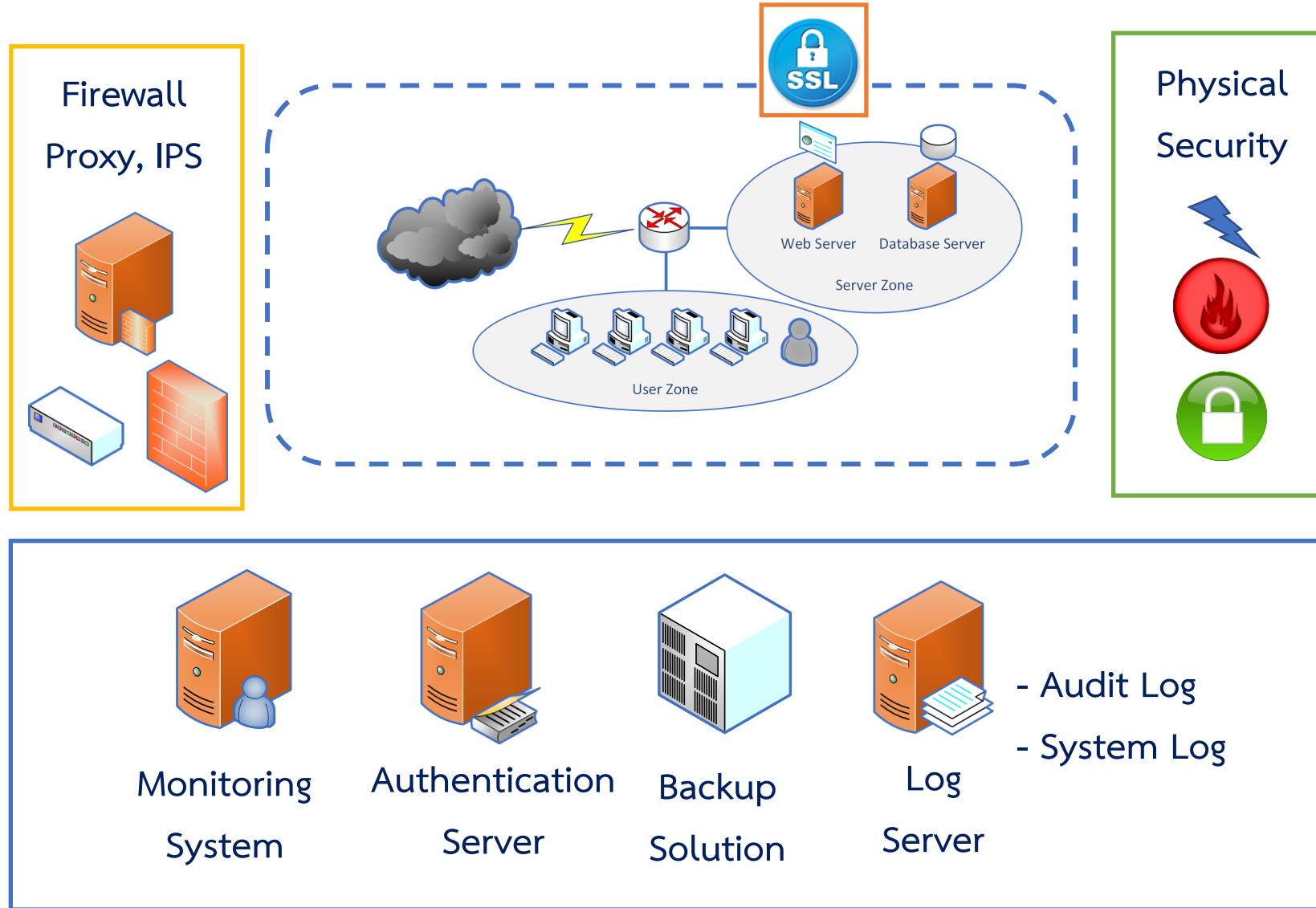
1. ข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ
 - บุคคลภายนอก
 - หน่วยงานภายนอก
2. เอกสาร Non-Disclosure Agreement
3. เอกสารบันทึกการทรมานสารสนเทศ
 - บันทึกให้ค้นหาได้



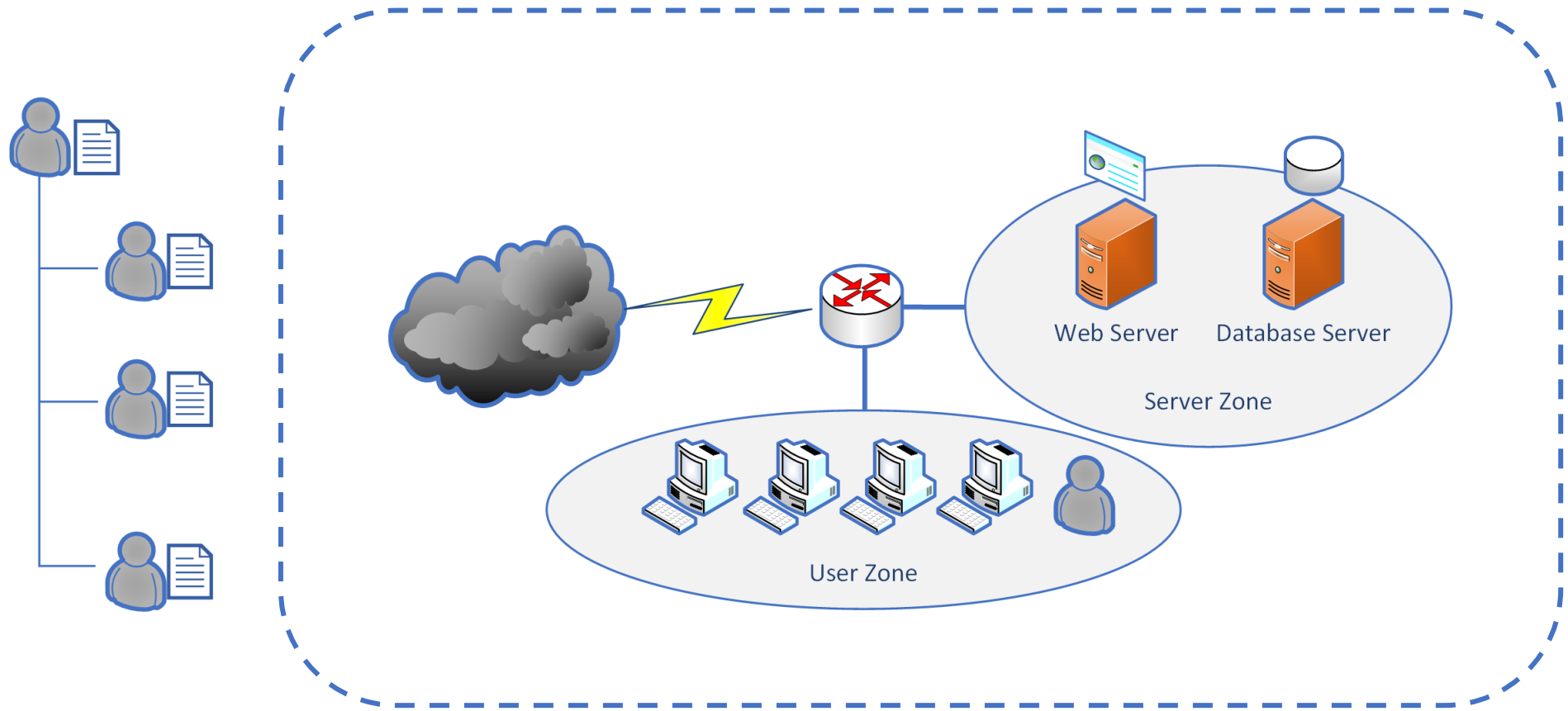
- จัดทำ ปรับปรุง ดูแล เอกสารขั้นตอนปฏิบัติงาน
- ตรวจสอบรายงาน / บันทึก การให้บริการบุคคลภายนอกอย่างสม่ำเสมอ
- ขั้นตอนตรวจ , ป้องกัน , กู้คืน กรณี มัลแวร์
- การสร้างความตระหนักรู้กับผู้ใช้งานกรณีมัลแวร์
- การสำรองข้อมูล / กู้คืนข้อมูล
- ทบทวนนโยบาย
- การควบคุม ดูแล ติดตาม การทำงานในการจ้างช่วง
- การซ้อมแผน Incident Response Process
- การซ้อมแผน BCP
- ป้องกันการใช้งานผิดวัตถุประสงค์
- การดูแลให้สอดคล้องกับกฎหมาย



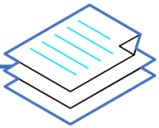
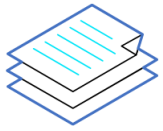
- การพิจารณา ทบทวน เพื่ออนุมัติติดตั้งระบบ
- กำหนดให้มีการ Sign NDA เมื่อดำเนินงานเกี่ยวกับระบบที่สำคัญหรือข้อมูลสำคัญ
- บันทึก Asset ให้ค้นหาภายหลังได้
- สอบทานข้อมูลสารสนเทศที่เผยแพร่สู่สาธารณะ
- ลงบัญชีผู้ใช้ / ยกเลิกบัญชีผู้ใช้
- การให้สิทธิการเข้าถึงระบบ / การเปลี่ยนแปลงสิทธิ
- จำกัดการเข้าถึงฟังก์ชัน ข้อมูล ระบบสารสนเทศ



มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบ
สารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง



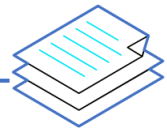
- กำหนดเนื่องานและความรับผิดชอบให้ชัดเจน



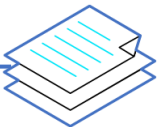
นโยบาย

นโยบาย

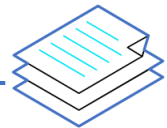
- คัดกรองข้อมูลส่วนบุคคล



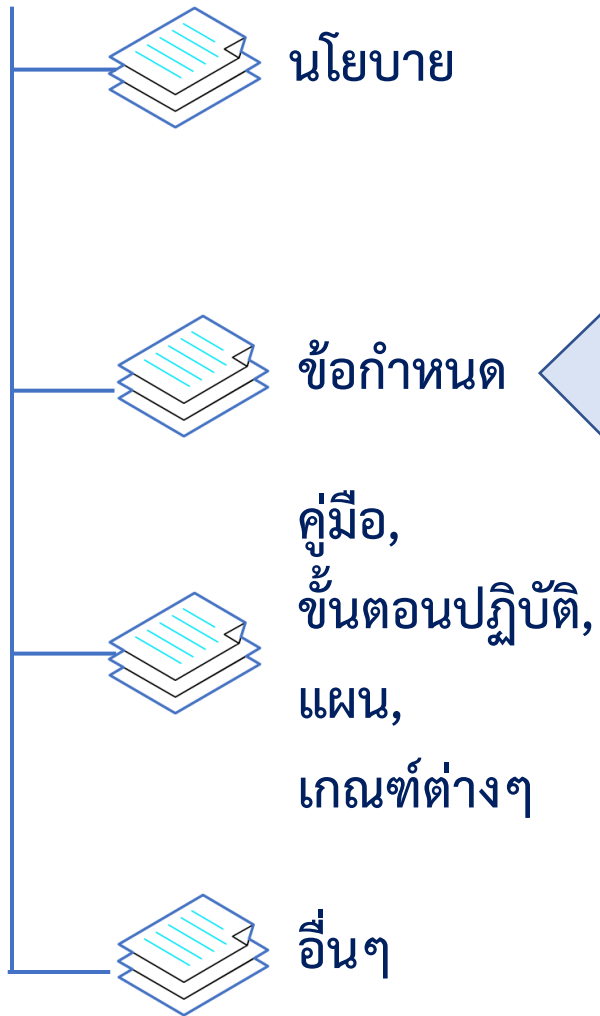
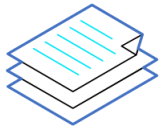
ข้อกำหนด



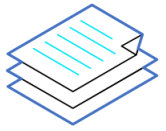
คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ



อื่นๆ



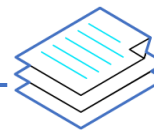
1. (เพิ่มเติม) ข้อกำหนดในการรักษาความมั่นคงปลอดภัย
 - ไม่นำอุปกรณ์ ข้อมูล ซอฟต์แวร์ ออกนอกพื้นที่
 - ให้ผู้ใช้งานใช้รหัสผ่านอย่างปลอดภัย
 - กำหนดวิธีการตรวจสอบตัวตนที่เหมาะสมในการเข้าถึงระบบจากระยะไกล
 - จำกัดการเข้าถึง source code ของโปรแกรม
 - เมื่อมีการเปลี่ยนแปลงใดๆ ให้ทบทวน/ทดสอบการทำงานของโปรแกรมสำคัญ
 - ป้องกันเครื่องมือที่ใช้เพื่อตรวจสอบระบบ
2. ข้อกำหนดขั้นตอนในการจำแนกประเภทข้อมูลสารสนเทศ
3. ข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ในภาวะฉุกเฉิน
4. ข้อกำหนดการตรวจสอบและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ



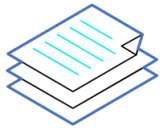
 นโยบาย

 ข้อกำหนด

 คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

 อื่นๆ

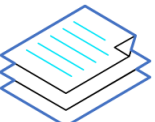
- ขั้นตอนปฏิบัติ
 - ในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะ
 - การจัดการและจัดเก็บข้อมูลสารสนเทศ
 - กำหนดขั้นตอนการ log-on ควบคุมการเข้าถึงระบบปฏิบัติการ
 - การเลือกชุดข้อมูลสารสนเทศที่จะนำไปทดสอบระบบ และควบคุมไม่ให้ข้อมูลรั่วไหล
 - ใช้การเข้ารหัสลับกับข้อมูลที่สอดคล้องกับข้อกำหนดต่างๆ
- กรอบงานหลักในการพัฒนา BCP



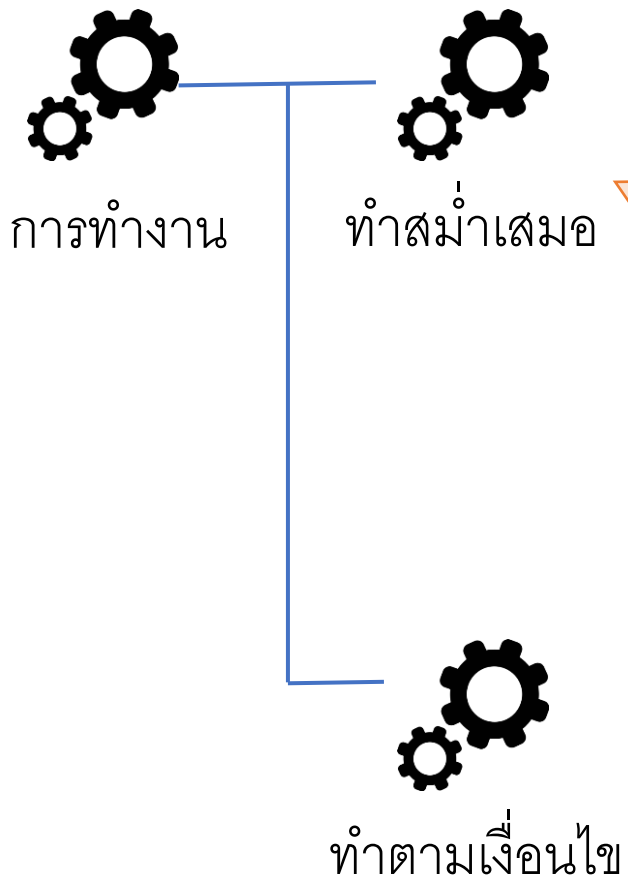
 นโยบาย

 ข้อกำหนด

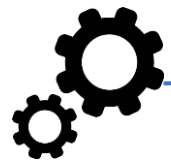
 คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

 อื่นๆ

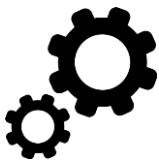
- เอกสารบันทึกรายการทรัพย์สินสารสนเทศ
 - บุคคลรับผิดชอบ
 - ระเบียบการใช้
 - จำแนกประเภทข้อมูล (มูลค่า,กฎหมาย,ชั้นความลับ,ความสำคัญ)
- เอกสารการจัดกลุ่มตามประเภทของข้อมูล ระบบสารสนเทศ กลุ่มผู้ใช้งาน



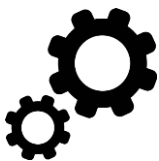
- ติดตามและประเมินผล
 - ขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยด้านสารสนเทศ
 - นโยบายในการรักษาความมั่นคงปลอดภัย
 - การใช้ทรัพยากรสารสนเทศ
- วางแผน
 - ทรัพยากรสารสนเทศในอนาคต
- ทบทวน
 - แนวทางการบริหารจัดการเกี่ยวกับความมั่นคงปลอดภัย
 - IRP, BCP
- อบรม
 - การสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัย
- สื่อสาร ประชาสัมพันธ์
 - นโยบาย , ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย
- จัดจ้าง
 - ตรวจสอบระบบสารสนเทศทางเทคนิค
- วิเคราะห์ข้อมูล Log file และแก้ไขข้อผิดพลาดต่างๆ



การทำงาน



ทำสม่ำเสมอ



ทำตามเงื่อนไข

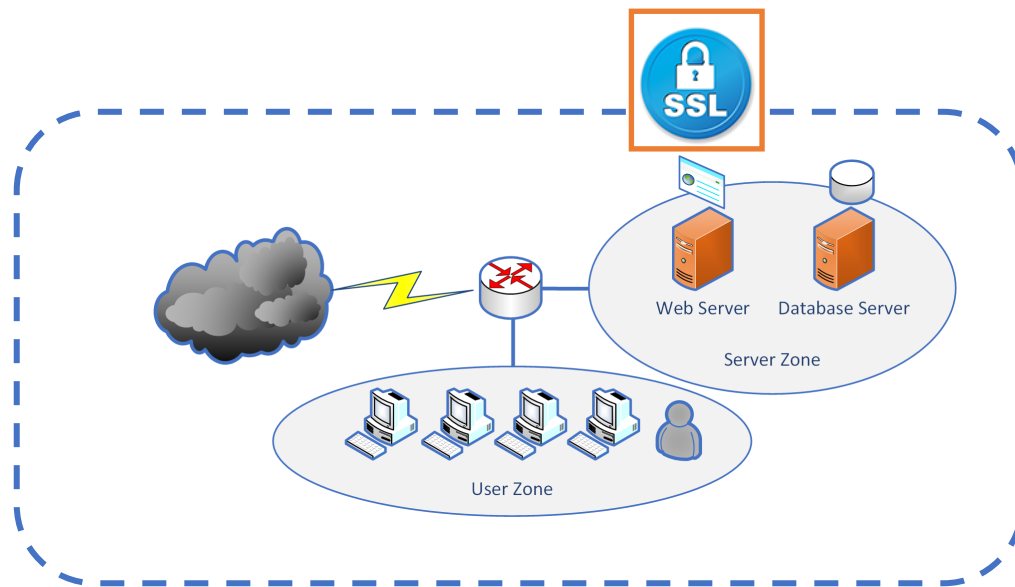
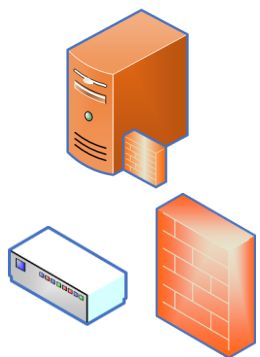
- การจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ
- ตรวจสอบข้อมูลใดๆ ที่รับเข้าสู่ Application
- ตรวจสอบข้อมูลใดๆ ที่เป็นผลลัพธ์จากการประมวลผลของ Application



Infrastructure

แบ่งแยกเครือข่ายผู้ใช้งาน
ควบคุมเส้นทางการไหลของข้อมูล

Firewall
Proxy, IPS



Physical
Security



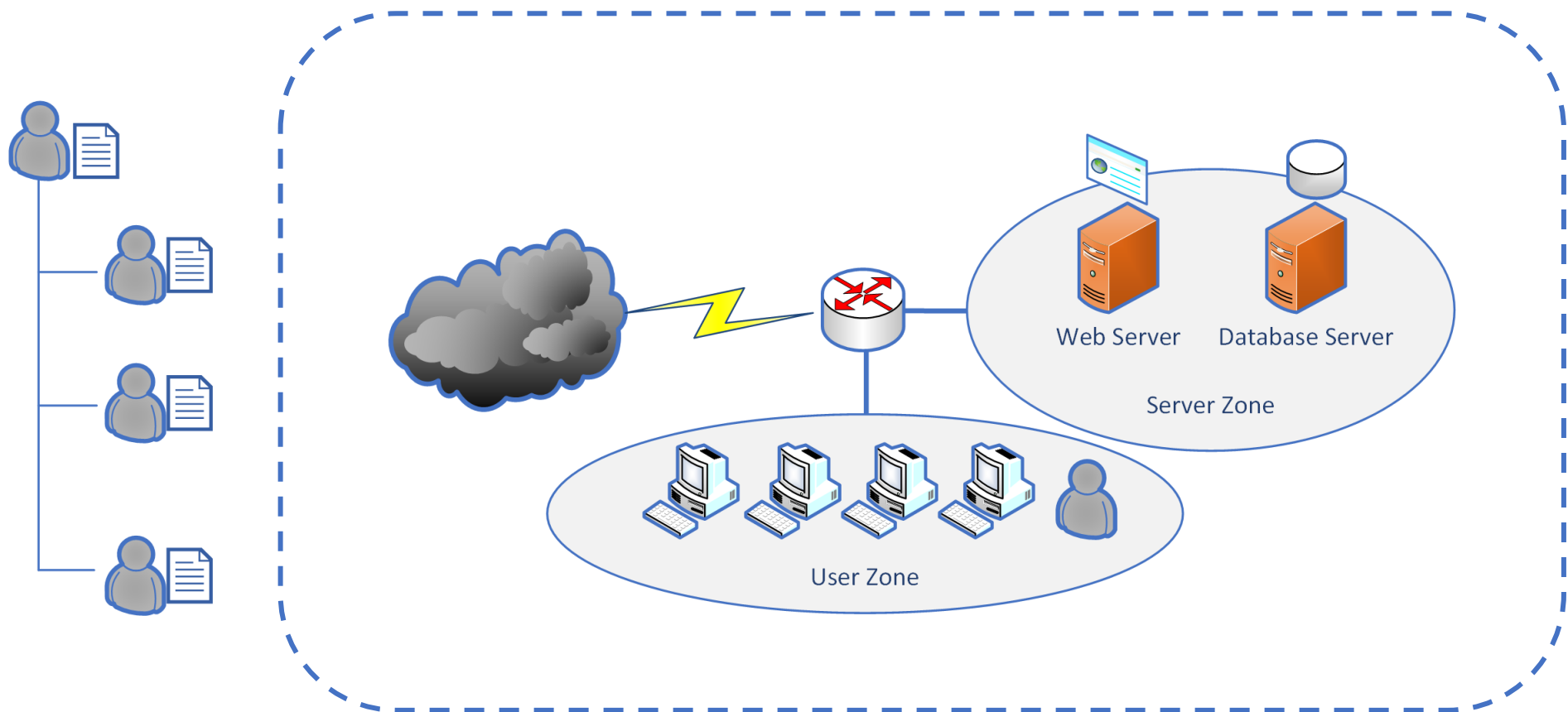
Key Management Remote Configuration Time Synchronization

Monitoring System Authentication Server Backup Solution Log Server

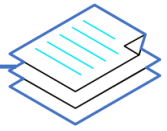
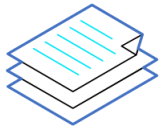
- Audit Log
- System Log

บริหารจัดการรหัสผ่านอัตโนมัติ

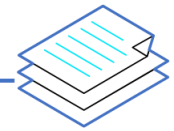
มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบ
สารสนเทศตามวิธีการแบบปลอดภัยในระดับ
เครื่องคิด



- กำหนดเนื่องานและความรับผิดชอบให้ชัดเจน



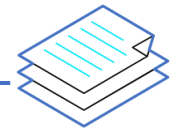
นโยบาย



ข้อกำหนด



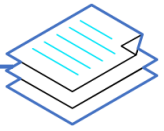
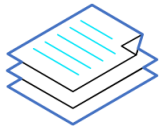
คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ



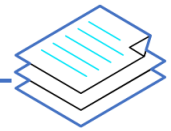
อื่นๆ

นโยบาย

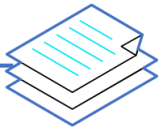
- แบ่งแยกหน้าที่ความรับผิดชอบ
- ห้ามใช้งาน mobile code
- Clear Desk
- Clear Screen
- ปฏิบัติงานจากนอกหน่วยงาน (Teleworking)
- การใช้งานทางเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ



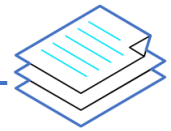
นโยบาย



ข้อกำหนด

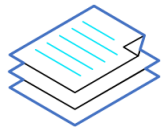


คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ



อื่นๆ

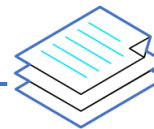
1. (เพิ่มเติม) ข้อกำหนดในการรักษาความมั่นคงปลอดภัย
 - การนำอุปกรณ์สารสนเทศไปใช้นอกสถานที่
 - ทำลายอุปกรณ์ / ข้อมูล ก่อนยกเลิก/จำหน่าย
 - ข้อกำหนดขั้นต่ำในการรักษาความถูกต้องแท้จริง / ครบถ้วนของข้อมูลใน Application
2. ข้อกำหนดในการรับพนักงานหรือจ้างบุคคลภายนอก
 - ตรวจสอบประวัติ คุณสมบัติ โดยคำนึงถึงชั้นความลับที่จะเข้าถึง และความเสี่ยง
3. ข้อกำหนดในการป้องกันเอกสารเกี่ยวกับระบบสารสนเทศ
4. กำหนดให้พนักงาน / ผู้ใช้งานจากภายนอก รายงานจุดอ่อนที่พบระหว่างการใช้งาน
5. ขอบเขตความรับผิดชอบของผู้บริหารและขั้นตอนปฏิบัติงานในสถานการณ์ที่ไม่พึงประสงค์



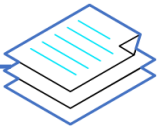
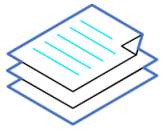
 นโยบาย

 ข้อกำหนด

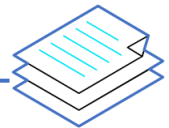
 คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

 อื่นๆ

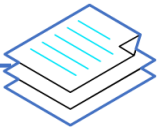
- ขั้นตอนปฏิบัติ
 - ขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอก
 - หน่วยงานกำกับดูแล หรือบังคับใช้กฎหมาย
 - หน่วยงานควบคุมดูแลสถานการณ์ฉุกเฉินต่างๆ
 - การใช้ / ทำลาย removable media
 - การเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสารสนเทศ
 - ป้องกันข้อมูลสารสนเทศที่สื่อสารผ่าน messaging , E-mail
 - การกำหนดรหัสผ่าน
 - การปฏิบัติงานจากนอกหน่วยงาน (Teleworking)
 - ควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ
 - การใช้ข้อมูลที่อาจเป็นทรัพย์สินทางปัญญา
 - การใช้งานซอฟต์แวร์ให้สอดคล้องกับข้อกำหนดตามสัญญาต่างๆ
- แนวทางการป้องกันทางกายภาพสำหรับพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย



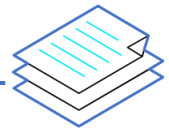
นโยบาย



ข้อกำหนด

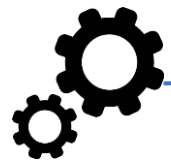


คู่มือ,
ขั้นตอนปฏิบัติ,
แผน,
เกณฑ์ต่างๆ

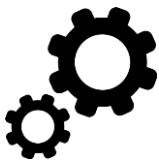


อื่นๆ

- เอกสารสัญญาจ้าง ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยไว้ในสัญญา



การทำงาน

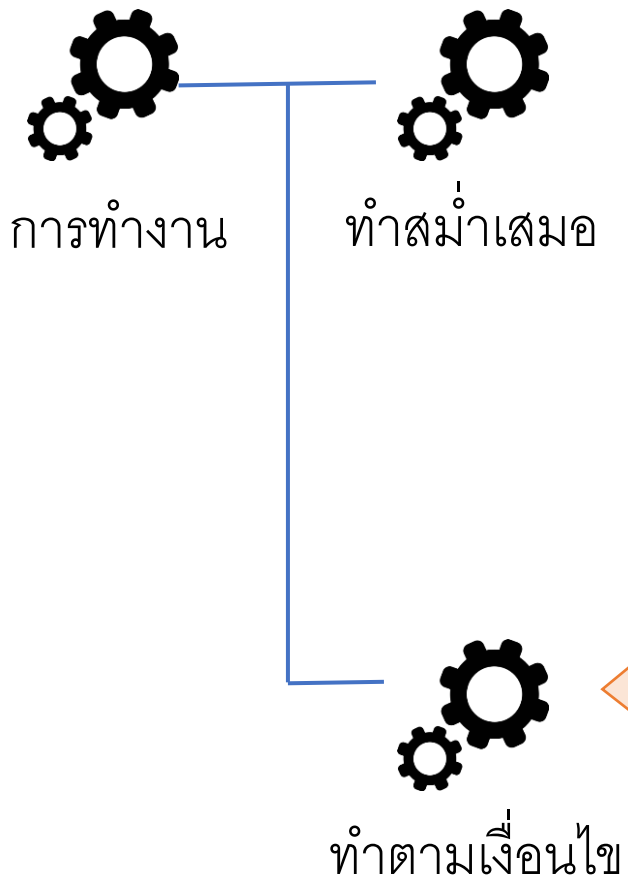


ทำสม่ำเสมอ



ทำตามเงื่อนไข

- บริหารจัดการการเปลี่ยนแปลง
- ปรับปรุงนโยบาย ขั้นตอนปฏิบัติ
- ผู้บริหารติดตามทบทวนสิทธิของผู้ใช้งานอย่างเป็นทางการ
- ควบคุมการเปลี่ยนแปลงต่างๆ ในการพัฒนาระบบสารสนเทศอย่างเป็นทางการ



- กิจกรรมสร้างความร่วมมือระหว่างผู้เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ
- ระบุความเสี่ยงที่อาจเกิดขึ้นก่อนอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ
- ตรวจสอบการทำงานของ Application เพื่อหาข้อผิดพลาด
- จำกัดการเปลี่ยนแปลงใดๆ ต่อซอฟต์แวร์ที่ใช้งาน
- กำหนดมาตรการเพื่อลดโอกาสการรั่วไหลของข้อมูล
- เมื่อมีเหตุไม่พึงประสงค์ที่เกี่ยวข้องกับกฎหมาย ให้มีการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมาย



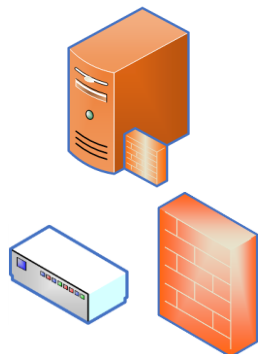
Infrastructure

ป้องกัน Mobile Code
ป้องกันการใช้ Utility
จำกัดระยะเวลาการเชื่อมต่อ

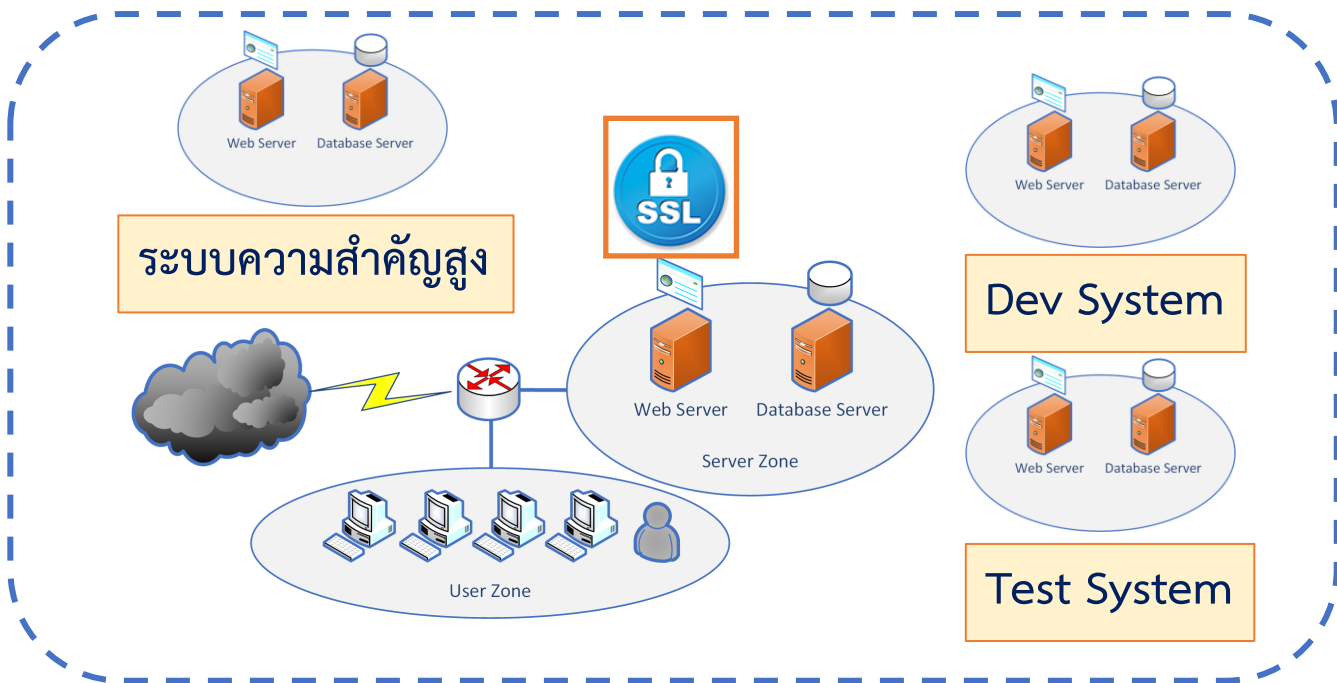
ป้องกันสาย Cable
ระบุอุปกรณ์ที่เชื่อมต่อโดยอัตโนมัติ

แบ่งแยกพื้นที่ของบุคคลภายนอกกับ
พื้นที่ของระบบสารสนเทศ
ควบคุมการเข้าออก

Firewall
Proxy, IPS



ระบบความสำคัญสูง



Physical
Security



Key Management
Remote Configuration
Time Synchronization

Monitoring System
Authentication Server
Backup Solution
Log Server
- Audit Log
- System Log