รอบรู้นโยบายความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยศรีนครินทรวิโรฒ

SWU Information Security

มหัทธวัฒน์ รักษาเกียรติศักดิ์
ผู้ช่วยผู้อำนวยการสำนักคอมพิวเตอร์

SWU IT Best practice

เนื้อหาที่จะนำเสนอ

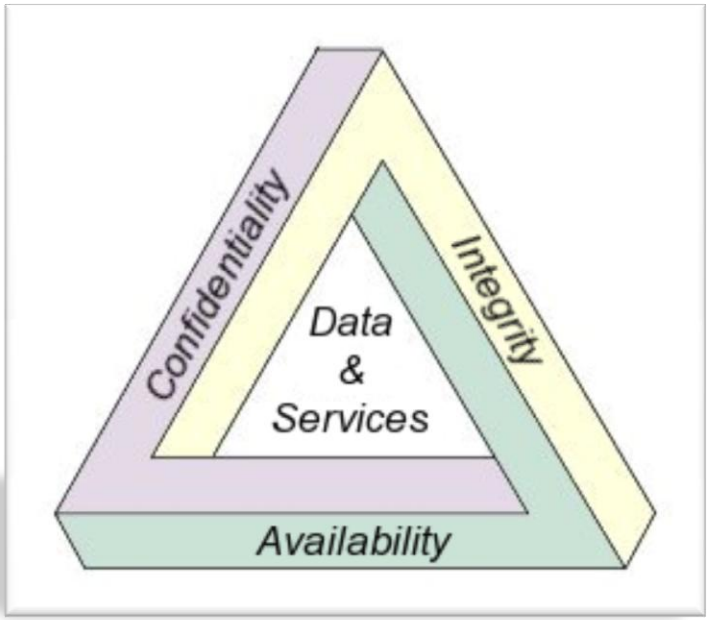
- ความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ
- ISO 27001
- นโยบายความมั่นคงปลอดภัยของสารสนเทศ
- แนวปฏิบัติด้านความมั่นคงปลอดภัยของสารสนเทศ
- ปัจจัยสู่ความสำเร็จ

ทำไมต้องสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

- ICT เป็นสิ่งแวดล้อมใหม่ในองค์กร
- ICT เป็นการเชื่อมโยงการทำงานของทุกคนเข้าด้วยกัน รวมทั้งเชื่อมโยงสู่โลกภายนอก
- ICT เป็นทรัพย์สินที่นับว่ามีคุณค่ายิ่งขององค์กร
- ICT มีภัยคุกคามที่นับวันจะซับซ้อนและทวีความรุนแรงมากยิ่งขึ้น

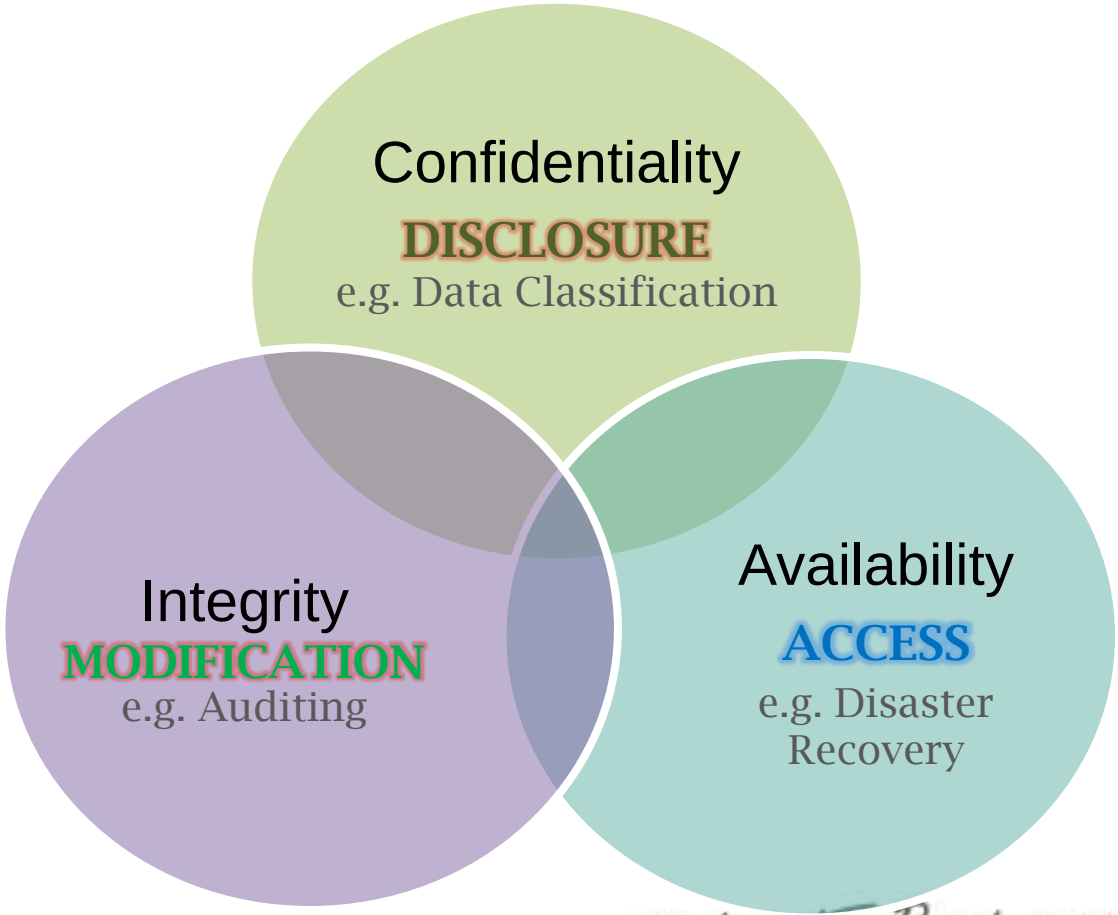
องค์ประกอบด้านความมั่นคงปลอดภัยของสารสนเทศ

- ความลับ (Confidentiality)
- ความคงสภาพ (Integrity)
- ความพร้อมใช้ (Availability)



The CIA triad

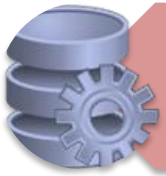
Classical Security Objectives



SWU IT Best practice

การรักษาความมั่นคงปลอดภัยของสารสนเทศ เกี่ยวข้องกับ ...

เทคโนโลยี



กระบวนการทำงาน

คน

การบริหารจัดการ

SWU IT Best practice

คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ

- องค์ประกอบ -

1. อธิการบดี
2. ที่ปรึกษาอธิการบดีด้านไอซีที
3. นายภิญโญ ตรีเพชรรภรณ์
4. ผู้อำนวยการสำนักคอมพิวเตอร์
5. ผู้อำนวยการสำนักหอสมุดกลาง
6. ผู้อำนวยการสำนักสื่อและเทคโนโลยีทางการศึกษา
7. อาจารย์อรรณพ โพธิสุข
8. อาจารย์สุคนธ์ อักษรชู
9. อาจารย์สมภพ รอดอัมพร
10. อาจารย์สุพิมพ์ วงษ์ทองแท้
11. อาจารย์วราภรณ์ วิยานนท์
12. อาจารย์ศุภชัย ไทยเจริญ
13. อาจารย์อาคม ม่วงเขาแดง
14. นายสมบุญ อุดมพรยิ่ง
15. นายดิเรก อึ้งตระกูล
16. นางสาววิลาวัลย์ บัวขำ
17. นายมหัทธวัฒน์ รักษาเกียรติศักดิ์
18. นายนคร บริพนธ์มงคล
19. นายสันติ สุขยานันท์
20. นางสาวพรทิพย์ พงษ์สวัสดิ์

คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ
- ภาระหน้าที่ -

- ร่าง กำกับ และดูแลนโยบายความมั่นคงปลอดภัยของสารสนเทศ
- ออกระเบียบและแนวปฏิบัติที่ดีในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย
- กำหนดขั้นตอนการดำเนินงานด้านความมั่นคงปลอดภัยของสารสนเทศตามแนวมาตรฐาน ISO 27002
- รณรงค์ให้หน่วยงานและผู้ใช้เข้าใจถึงนโยบายความมั่นคงปลอดภัยของสารสนเทศ
- รายงานข้อมูลการดำเนินงานต่อคณะกรรมการบริหารยุทธศาสตร์ไอซีทีและการศึกษาไซเบอร์และมหาวิทยาลัย
- ประเมินผลการดำเนินงานเพื่อพัฒนาแนวปฏิบัติที่ดีของการใช้สารสนเทศของนิสิต คณาจารย์ บุคลากร และหน่วยงานต่าง ๆ

แนวทางการรักษาความมั่นคงปลอดภัย

- มาตรฐานสากลในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

International Standards

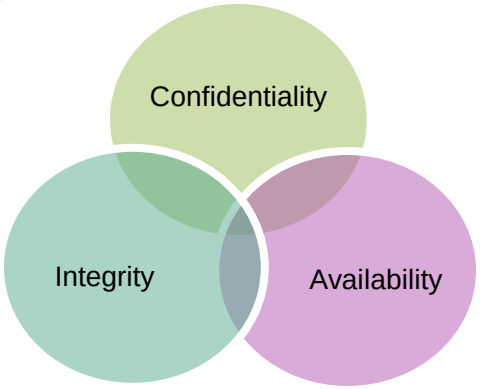
- **COBIT**
  - Control OBjectives for Information Technology
- **ITIL**
  - Information Technology Infrastructure Library
- **ISO/IEC 27001**
  - Information Security Standard

ISO/IEC 27001

- มาตรฐานระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS : Information System Management System)

- เน้นความสำคัญของกระบวนการตามแนวทางวงจรคุณภาพ

- เน้นจัดการใน 3 องค์ประกอบด้านความมั่นคงปลอดภัยของสารสนเทศ

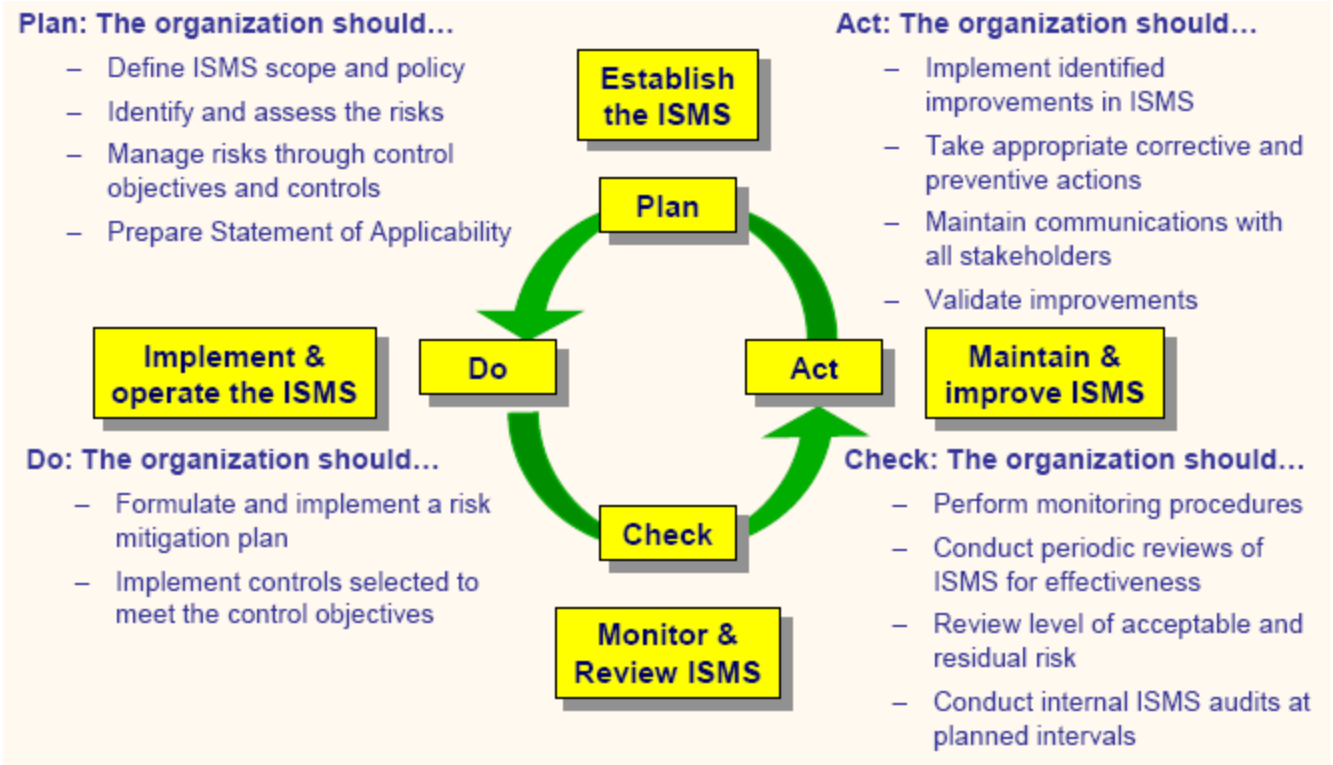


ISO/IEC 27001

ข้อดีของการนำไปใช้

- มาตรฐานสากลที่เป็นที่ยอมรับในวงกว้าง
- มาตรฐานที่ไม่ผูกติดกับผลิตภัณฑ์
- มาตรฐานเพื่อการตรวจประเมินและรับรอง
- แหล่งอ้างอิงที่ครบถ้วน - องค์ความรู้ หนังสือ การสัมมนา ที่ปรึกษาและผู้เชี่ยวชาญ

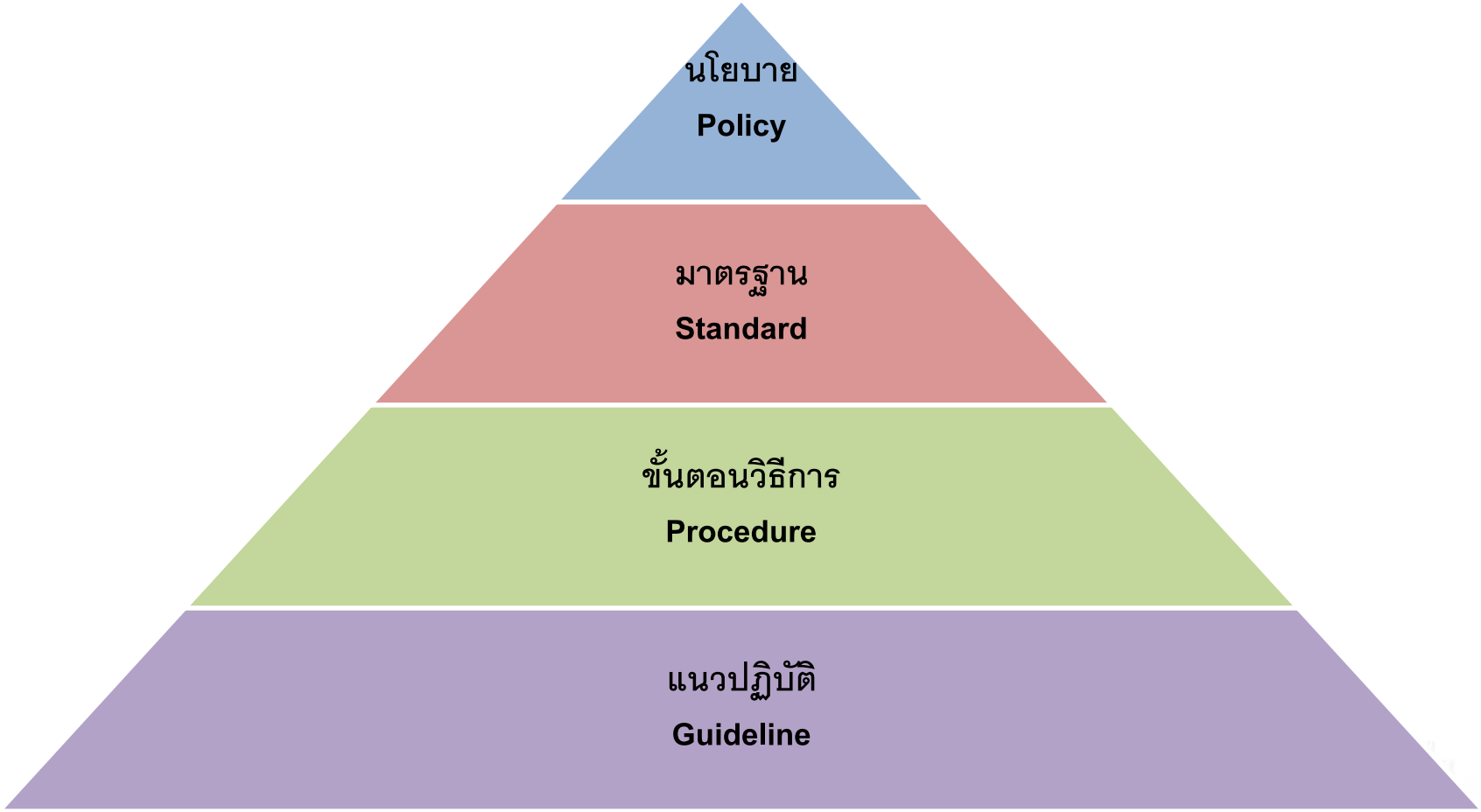
แนวทางการดำเนินการของ ISO/IEC 27001



พันธกิจที่สำคัญของคณะกรรมการ

- พัฒนา นโยบาย มาตรฐาน ขั้นตอนวิธีการ และแนวปฏิบัติ
- ตรวจประเมินและจัดการความเสี่ยง
- พัฒนากลไกการตอบสนองต่อเหตุการณ์ความเสี่ยงที่เกิดขึ้น
- สร้างความรับผิดชอบของทุกคนในองค์กรเพื่อให้ปฏิบัติตามนโยบาย

ลำดับชั้นเอกสารจากนโยบายสู่แนวปฏิบัติ



พันธกิจที่สำคัญ

นโยบาย

- ข้อกำหนดระดับสูงของมหาวิทยาลัย
- กำหนดขึ้นเพื่อใช้ในการขับเคลื่อน หรือ ตัดสินใจภายในมหาวิทยาลัย
- อยู่ภายใต้กระบวนการตรวจสอบอย่างเข้มงวด

POLICY

พันธกิจที่สำคัญ

มาตรฐาน

- ข้อกำหนดความต้องการขั้นต่ำที่จะสามารถปฏิบัติได้ตามนโยบาย
- กำหนดขึ้นเพื่อจำกัด หรือ หลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้น
- กำหนดขึ้นเพื่อให้ทุกคนสามารถปฏิบัติตามกฎหมาย และกฎระเบียบของมหาวิทยาลัย
- ผ่านกระบวนการตรวจประเมินเพื่อการพัฒนา

STANDARD

SWU IT Best practice

พันธกิจที่สำคัญ

ขั้นตอนวิธีการ

- ข้อกำหนดที่เป็นลำดับขั้นตอนของวิธีการปฏิบัติเพื่อให้เกิดสัมฤทธิผลในการทำงาน

PROCEDURE

SWU IT Best practice

พันธกิจที่สำคัญ

แนวปฏิบัติ

- ข้อปฏิบัติและคำแนะนำที่ดีเพื่อให้บรรลุวัตถุประสงค์ของการใช้งาน
- ข้อปฏิบัติเชิงเทคนิคที่ขึ้นกับเทคโนโลยีที่มหาวิทยาลัยเลือกใช้
- ปรับปรุงอย่างต่อเนื่องเพื่อให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลง

GUIDELINE

SWU IT Best practice

รายละเอียดเกี่ยวกับ

ISO 27001

- A.5 Security Policy
- A.6 Organization of information security
- A.7 Asset management
- A.8 Human resources security
- A.9 Physical and environmental security
- A.10 Communications and operations management
- A.11 Access control
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management
- A.14 Business continuity management
- A.15 Compliance

การดำเนินการของมหาวิทยาลัย

ISO 27001

- A.5 Security Policy
- A.6 Organization of information security
- A.7 Asset management
- A.8 Human resources security
- A.9 Physical and environmental security
- A.10 Communications and operations management
- A.11 Access control
- A.12 Information systems acquisition, development and maintenance
- A.13 Information security incident management
- A.14 Business continuity management
- A.15 Compliance

SWU Information Security Policy

- หมวด 1 นโยบายความมั่นคงปลอดภัย
- หมวด 2 โครงสร้างการบริหารความมั่นคงปลอดภัยสารสนเทศ
- หมวด 3 การจัดการทรัพย์สินสารสนเทศ
- หมวด 4 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร
- หมวด 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวด 6 การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ
- หมวด 7 การควบคุมการเข้าถึง
- หมวด 8 การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ
- หมวด 9 การดำเนินการกับเหตุการณ์ด้านความมั่นคงปลอดภัย
- หมวด 10 การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย
- หมวด 11 การปฏิบัติตามข้อกำหนด

หมวด 1 นโยบายความมั่นคงปลอดภัย

Security Policy

- ควรอัพเดตประมาณปีละครั้ง (Signed by CIO)
- ทบทวนทุกไตรมาส (ISM Committee)

All SWU Staff

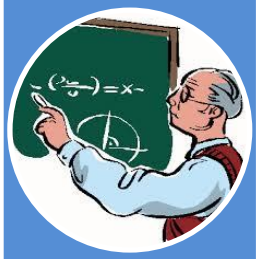
Drafted → **Revised** → **Approved** → **Public**

Drafted	Revised	Approved
คณะทำงานด้านการรักษาความมั่นคงปลอดภัย	คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

หน้าที่ความรับผิดชอบ

- คณะทำงานการรักษาความมั่นคงปลอดภัย - ร่างนโยบาย และระเบียบในการดำเนินการด้านนโยบายความมั่นคงปลอดภัยสารสนเทศ
- คณะกรรมการบริหารความมั่นคงปลอดภัยของสารสนเทศ (ISMC) - เข้าตรวจสอบดูความเหมาะสมของเนื้อหา และทบทวนการอัพเดตสิ่งต่าง ๆที่เกิดขึ้นหลังจากที่มีการใช้นโยบายไปแล้ว
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง – ผู้อนุมัตินโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- นิสิต อาจารย์ บุคลากร - รับทราบ และปฏิบัติตามกรอบที่องค์กรระบุไว้

การใช้งานที่ยอมรับได้ (Acceptable Use Policy)



การเรียนการสอน

การวิจัย

การบริหารงานตามภารกิจของมหาวิทยาลัย

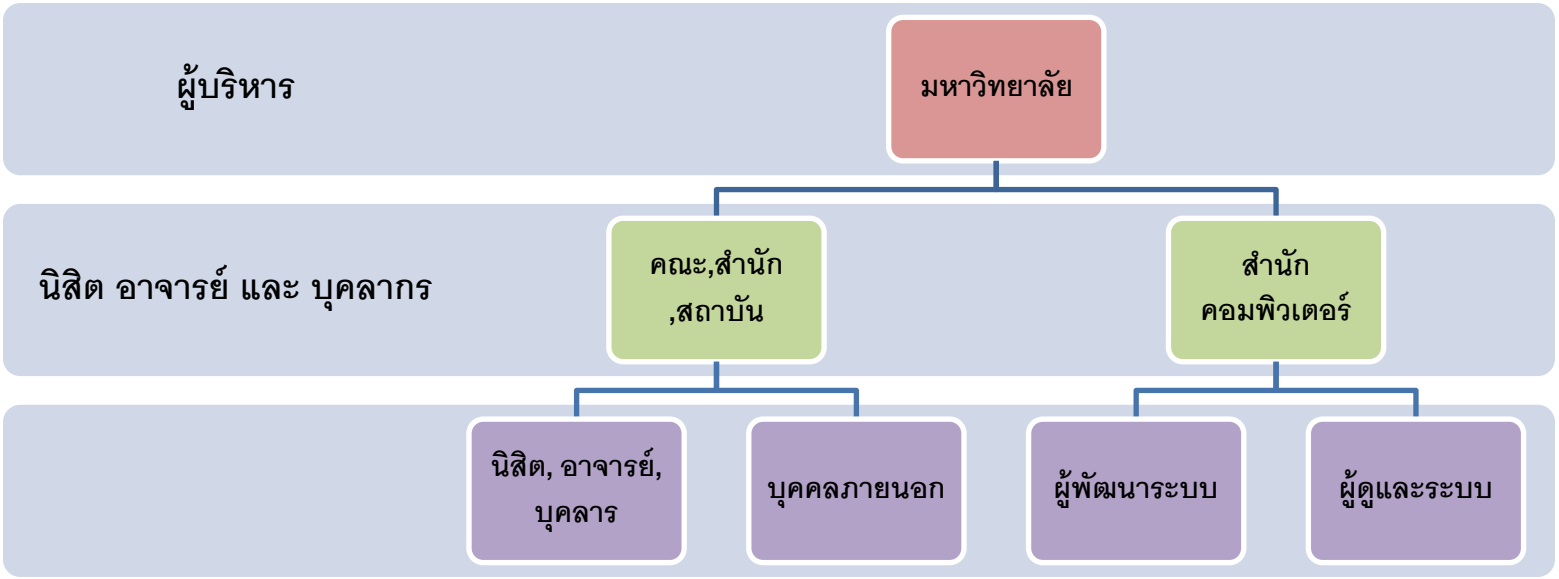
การพัฒนาการเรียนรู้ส่วนบุคคล

การให้คำแนะนำปรึกษาซึ่งเป็นงานตามข้อสัญญาหรือข้อตกลงกับมหาวิทยาลัย

การติดต่อสื่อสารตามวัตถุประสงค์ดังกล่าวข้างต้น

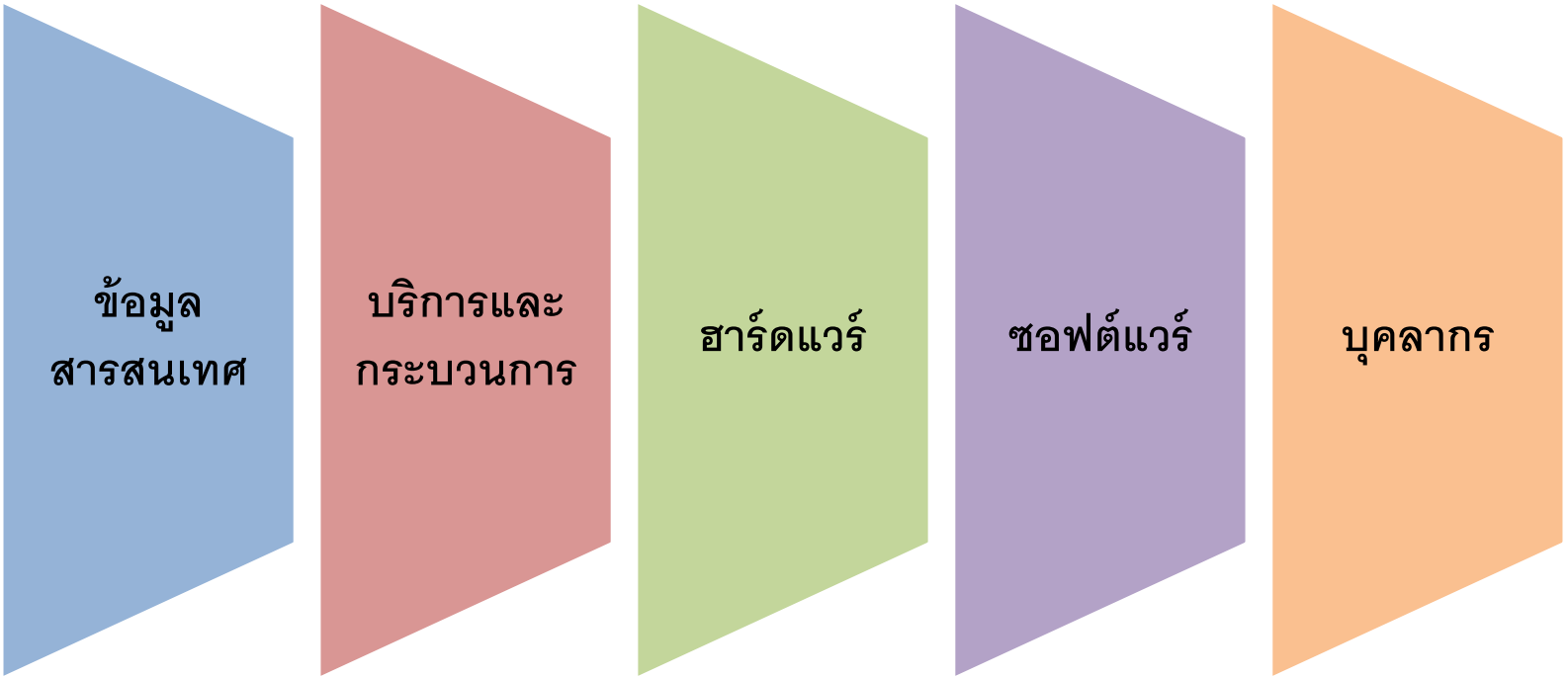
หมวด 2 โครงสร้างการบริหารความมั่นคงปลอดภัยสารสนเทศ

Organization of Information Security



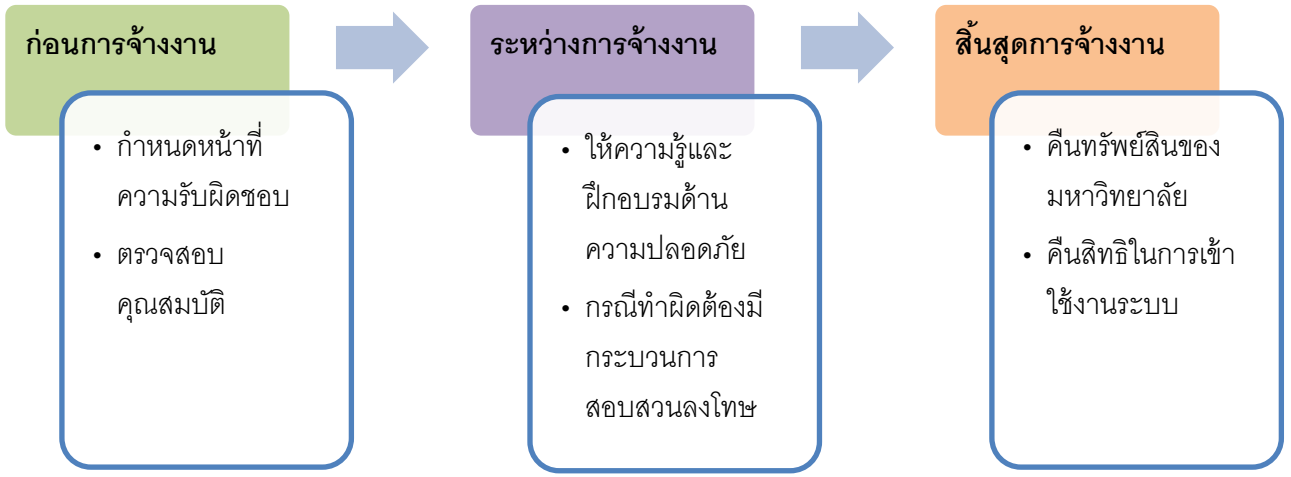
หมวด 3 การจัดการทรัพย์สินสารสนเทศ

Asset Management



หมวด 4 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

Human Resources Security



หมวด 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

Physical and environmental security

การรักษาความปลอดภัยทางกายภาพ

การควบคุมการเข้าถึงอุปกรณ์

การรักษาความปลอดภัยของอุปกรณ์

การนำอุปกรณ์ออกนอกหน่วยงาน

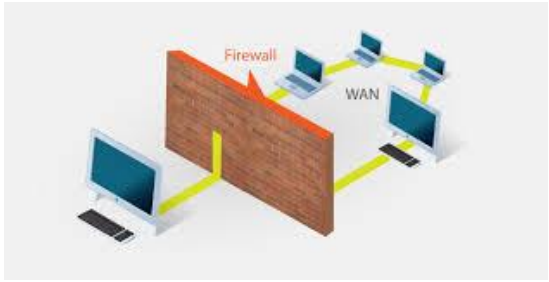
หมวด 6 การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ

Communications and operations management

กำหนดความรับผิดชอบ	การรับบริการจากหน่วยงานภายนอก	การวางแผนและตรวจรับทรัพยากรสารสนเทศ
การป้องกันโปรแกรมที่ไม่ประสงค์ดี	การสำรองข้อมูล	การเฝ้าระวังด้านความมั่นคงปลอดภัย

หมวด 7 การควบคุมการเข้าถึง

Access Control



SWU IT Best practice

หมวด 8 การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

Information systems acquisition, development and maintenance

ข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศ

การตรวจสอบประมวลผล

สร้างความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ

สร้างความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบ

การจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

SWU IT Best practice

หมวด 9 การดำเนินการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

Information security incident management

รายงานเหตุการณ์และจุดอ่อนด้านความปลอดภัย

การจัดการและแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

SWU IT Best practice

หมวด 10 การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย

Business continuity management

- ประเด็นความสูญเสียที่เกิดขึ้น

พื้นที่ใช้งานหลักภายในอาคาร

- ห้องปฏิบัติการระบบเครือข่าย

อาคารหลัก

- อาคาร **16** สำนักคอมพิวเตอร์

พื้นที่ปฏิบัติงานหลัก

- ห้องคอมพิวเตอร์กลาง **Data Center**

ระบบเครือข่ายหลัก

- การออก **internet,** เครือข่ายบัวศรี

บุคลากรหลัก

- ผู้ดูแลระบบหลักของมหาวิทยาลัย

หมวด 11 การปฏิบัติตามข้อกำหนด

Compliance

- กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการกระทำธุรกรรมทางอิเลกทรอนิกส์

พระราชบัญญัติว่าด้วย
ธุรกรรมทาง
อิเล็กทรอนิกส์ พ.ศ. 2544

พระราชกฤษฎีกากำหนด
หลักเกณฑ์และวิธีการใน
การทำธุรกรรม
อิเล็กทรอนิกส์ภาครัฐ
พ.ศ. 2549

พระราชบัญญัติว่าด้วยการ
กระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ. 2550

แนวปฏิบัติ

Guideline

- การบริหารจัดการด้านความมั่นคงปลอดภัย
- การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงของสารสนเทศ
- การจัดการด้านวินัยเมื่อมีการละเมิดหรือละเลย
- การควบคุมการเข้าออกห้องคอมพิวเตอร์กลาง
- การควบคุมการเข้าถึงระบบ
- การติดตั้งสวิชต์และฮับ
- การจัดการไฟร์วอลล์
- การจัดการเครือข่ายไร้สาย
- การป้องกันไวรัสคอมพิวเตอร์
- การบริหารจัดการสิทธิใช้งานระบบและการแบ่งแยกเครือข่าย
- การติดตั้งโทรศัพท์แบบวอยซ์โอเวอร์ไอพี
- การเฝ้าระวังระบบคอมพิวเตอร์และเครือข่าย
- การติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย
- การบริหารจัดการเครื่องแม่ข่ายสำหรับเว็บ
- การตั้งค่าเวลาของระบบโดยอิงมาตรฐานเวลาเดียวกัน
- การบำรุงรักษาเครื่องแม่ข่าย
- การสำรองและกู้คืนข้อมูล
- การบริหารจัดการระบบฐานข้อมูล
- การพัฒนาระบบสารสนเทศ
- การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ
- การจัดทำแผนสำรองด้านเทคโนโลยีสารสนเทศ
- การบริหารจัดการชื่อและรหัสผ่าน
- การใช้งานระบบสารสนเทศ
- การใช้งานจดหมายอิเล็กทรอนิกส์
- ความมั่นคงปลอดภัยของการใช้อินเทอร์เน็ต
- การติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย
- การใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

SWU IT Best practice

แนวปฏิบัติการบริหารจัดการชื่อและรหัสผ่าน

- ความจำเป็นของแนวปฏิบัติ
- คำถามที่พบบ่อย
  - เปลี่ยน password ทำอย่างไร
  - ถ้าไม่เปลี่ยนแล้วจะเป็นอย่างไร
  - เปลี่ยนบ่อยจำไม่ได้ (ขอจดก่อน)

แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

- ความจำเป็นของแนวปฏิบัติ
- คำถามที่พบบ่อย
  - Mail สอบถาม username และ password มาจากสำนักคอมพิวเตอร์หรือไม่
  - การ forward รูปภาพหรือ link ที่ทำให้ผู้อื่นเกิดความเสียหายจะมีความผิดหรือไม่
  - นำ e-mail ของมหาวิทยาลัยไปสมัครสมาชิกตามเว็บไซต์ต่างๆได้หรือไม่
  - ใช้งานเสร็จไม่ logout ได้หรือไม่
  - ทำไมรับ-ส่งจดหมายไม่ได้

แนวปฏิบัติความมั่นคงปลอดภัยของการใช้อินเทอร์เน็ต

- ความจำเป็นของแนวปฏิบัติ
- คำถามที่พบบ่อย
  - ถ้ามีการ post ข้อความที่ไม่สุภาพหรือทำให้ผู้อื่นเสียหายทางมหาวิทยาลัยมีการเก็บข้อมูลหรือไม่
  - ทำไมเครื่องคอมพิวเตอร์เครื่องของตนเองไม่สามารถใช้งานได้ในขณะที่เครื่องอื่นในห้องสามารถใช้งานได้
  - ถ้ามีการกระทำความผิดเกิดขึ้นผู้ที่รับผิดชอบจะเป็นใคร

แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

- ความจำเป็นของแนวปฏิบัติ
- คำถามที่พบบ่อย
  - จำเป็นต้องติดตั้ง antivirus หรือไม่
  - จำเป็นต้อง update patch หรือไม่
  - สามารถติดตั้งซอฟต์แวร์ที่ download มาจาก internet ได้หรือไม่

SWU IT Best practice

ปัจจัยสู่ความสำเร็จ

- ความร่วมมือของบุคลากรทุกคน
  - ต้องมีความเชื่อ เพื่อนำไปสู่ทัศนคติในเชิงบวก และส่งผลให้เกิดพฤติกรรมออกมาในที่สุด
- การให้ความรู้ ความตระหนักในประโยชน์
  - การทำจากความเข้าใจของตนเอง ไม่ได้เกิดจากการบังคับให้ทำโดยไม่มีความเข้าใจ
- การสนับสนุนจากผู้บริหาร
  - การกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด
- การกำหนดขอบเขต
  - เริ่มจากขอบเขตเล็ก ๆ ก่อนแล้วค่อยขยายเพิ่มเติม

THE KEY TO SUCCESS

SWU IT Best practice

ปัจจัยสู่ความสำเร็จ

- การสื่อสาร
  - ผู้เกี่ยวข้องทุกคนมีการติดต่อและรับทราบข้อมูลใหม่ๆอยู่เสมอ
- การประเมินความเสี่ยง
  - มีเครื่องมือที่เหมาะสมในการประเมินความเสี่ยง
- ระบบการจัดการเอกสาร
  - มีรูปแบบที่เป็นระเบียบและสืบค้นเข้าถึงได้ง่าย

THE KEY TO SUCCESS

SWU IT Best practice

Q & A

SWU IT Best practice