QA NEWS สจพ. NEWS
ข่าวประกันคุณภาพการศึกษา พระจอมเกล้าพระนครเหนือ
ศูนย์ประกันคุณภาพการศึกษา สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ
QA-KMITNB Website: http//qa.kmitnb.ac.th
ฉบับที่ 162 ปักษ์หลัง กุมภาพันธ์ พ.ศ. 2551

การจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ

ในยุคสังคมสารสนเทศปัจจุบัน ข้อมูลและสารสนเทศต่าง ๆ จัดว่าเป็นสินทรัพย์ขององค์กรเช่นกัน สินทรัพย์ในความหมายของสารสนเทศเป็นได้ทั้ง Hardware Software Application สิ่งพิมพ์ เอกสาร สื่ออิเล็กทรอนิกส์ รวมไปถึงตัวบุคคล สินทรัพย์เหล่านี้มีความสำคัญที่องค์กรต้องจัดการระวังป้องกันความเสียหายที่อาจเกิดขึ้น

การประกันคุณภาพสถาบันอุดมศึกษา ทั้งการประกันคุณภาพภายใน และการประเมินคุณภาพภายนอก ต่างก็เห็นความสำคัญของระบบความปลอดภัยของสารสนเทศต่อการดำเนินงานของสถาบันอุดมศึกษา สำนักงานคณะกรรมการการอุดมศึกษา และสำนักงานรับรองมาตรฐานและประเมินคุณภาพการศึกษา (องค์การมหาชน) จึงได้กำหนดให้มีการดำเนินการและประเมินเกี่ยวกับการจัดการรักษาความปลอดภัยของระบบฐานข้อมูล QA NEWS ฉบับนี้จึงนำแนวคิดของระบบ ISO 27001 ซึ่งเป็นระบบบริหารความมั่นคงปลอดภัยของข้อมูลในระดับสากลมานำเสนอเพื่อเป็นแนวทางในการจัดการรักษาความปลอดภัยของระบบฐานข้อมูลต่อไป

ในระดับสากลมีมาตรฐานและหลักปฏิบัติในการป้องกันและควบคุมข้อมูล คือ ระบบมาตรฐานด้านความปลอดภัยของข้อมูล ISO 27001 : 2005 (Information Security Management System : ISMS) ที่จะสร้างความมั่นใจว่าข้อมูลและสารสนเทศยังถูกเก็บรักษาอยู่ครบถ้วนปลอดภัย

ข้อกำหนดต่าง ๆ ของระบบ ISMS กำหนดขึ้นโดย ISO (The International Organization for Standardization) และ IEC (The Internal Electrotechnical Commission) หลักการของระบบ ISMS ยึดรูปแบบของวงจร PDCA (Plan Do Check Action) ISMS เป็นระบบการจัดการความปลอดภัยของข้อมูลที่มีวัตถุประสงค์เพื่อ

1. Confidentiality ให้แน่ใจว่าข้อมูลต่าง ๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิที่จะเข้าเท่านั้น
2. Integrity ป้องกันให้ข้อมูลมีความถูกต้อง และมีความสมบูรณ์
3. Availability ให้แน่ใจว่าผู้ที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้เมื่อมีความต้องการ

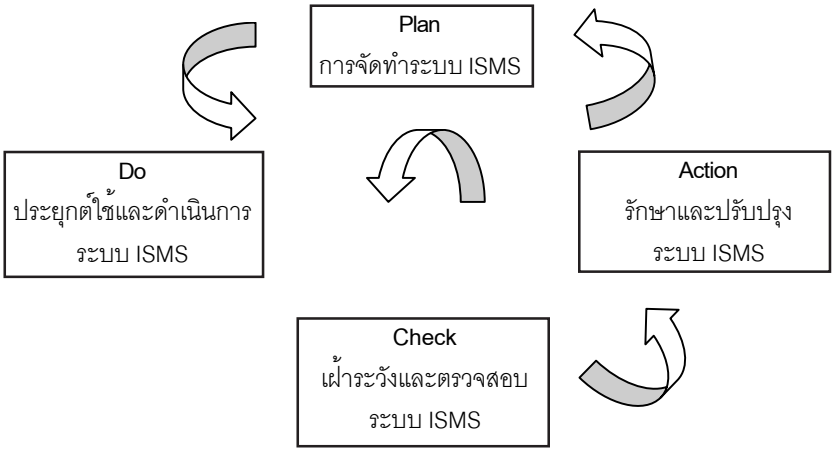
ระบบ ISMS เป็นระบบที่ Dymamic ระบบจะมีการหมุนเพื่อปรับปรุงอย่างต่อเนื่องอยู่ตลอดเวลาไม่มีที่สิ้นสุด โครงสร้างของข้อกำหนดจะถูกแบ่งตามวงจร PDCA ดังนี้

Plan : การจัดทำระบบ ISMS

1. กำหนด Scope และขอบเขตการจัดทำระบบ ISMS
2. กำหนดนโยบาย ISMS
3. กำหนดรูปแบบการประเมินความเสี่ยง
4. กำหนดความเสี่ยง
5. วิเคราะห์และประเมินความเสี่ยง
6. กำหนดและประเมินวิธีการเพื่อลดความเสี่ยง
7. เลือกการควบคุมเพื่อลดความเสี่ยง
8. เห็นชอบความเสี่ยงที่เหลืออยู่โดยฝ่ายบริหาร
9. เห็นชอบและประยุกต์ใช้ระบบโดยฝ่ายบริหาร
10. จัดทำ Statement of Application (SOA)

Do : ประยุกต์ใช้และดำเนินการระบบ ISMS

1. กำหนดแผนการลดความเสี่ยง
2. ดำเนินการตามแผนลดความเสี่ยง
3. ดำเนินการตามการควบคุมเพื่อลดความเสี่ยงที่เลือก



4. กำหนดการวัดประสิทธิภาพของระบบการควบคุม

5. จัดทำรายการฝึกอบรม

6. จัดการประยุกต์ใช้ระบบ

7. ประยุกต์ใช้ระเบียบปฏิบัติงาน

Check : **เฝ้าระวังและตรวจสอบระบบ** ISMS

1. จัดทำระเบียบปฏิบัติการเฝ้าระวังและตรวจสอบระบบ ISMS

2. ทบทวนประสิทธิภาพของระบบอย่างสม่ำเสมอ

3. วัดประสิทธิภาพการควบคุมในการปฏิบัติตามข้อกำหนด

4. ทบทวนการประเมินความเสี่ยงตามแผนความเสี่ยงที่เหลือ ระบบการประเมินความเสี่ยง และการเปลี่ยนแปลงต่าง ๆ ตามรอบระยะเวลาที่กำหนด

5. ดำเนินการตรวจติดตามภายในระบบ ISMS

6. ดำเนินการจัดทำการทบทวนโดยฝ่ายบริหาร

7. ปรับปรุงแผนความปลอดภัยให้ทันสมัย

8. บันทึกการทำงานและหลักฐานที่มีผลต่อประสิทธิภาพและประสิทธิผลของระบบ

Action : **รักษาและปรับปรุงระบบ** ISMS

1. ดำเนินการการแก้ไขสิ่งที่ไม่เป็นไปตามข้อกำหนด (Corrective Action) และการปฏิบัติการป้องกัน (Preventive Action)

2. สื่อสารวิธีการและการปรับปรุงต่าง ๆ ให้กับผู้ที่เกี่ยวข้อง

3. แน่ใจว่าวิธีการที่ปรับปรุงขึ้นบรรลุจุดประสงค์ที่วางไว้

สุวรรณา เอื้อสิทธิชัย ได้กล่าวถึงการดำเนินการจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศไว้ในบทความเรื่อง ISO 27001 เริ่มต้นอย่างไรดี ลงพิมพ์ในจุลสาร Productivity Corner ปีที่ 8 ฉบับที่ 93 ประจำเดือนธันวาคม 2550 ว่าอาจดำเนินการตามขั้นตอนดังนี้

1. กำหนดกระบวนการทางธุรกิจ โดยพิจารณาจากวัตถุประสงค์ของธุรกิจ วิสัยทัศน์ และพันธกิจขององค์กร เพื่อให้เห็นภาพรวมของกระบวนการและหน่วยงานต่าง ๆ

2. กำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง ซึ่งอาจเลือกทำเพียงบางส่วนเป็นการนำร่องก่อน การกำหนดหน่วยงานให้พิจารณาจากความสำคัญที่มีต่อธุรกิจ

3. กำหนดนโยบายความมั่นคงปลอดภัยขององค์กร

4. กำหนดแนวทางประเมินความเสี่ยง

5. วิเคราะห์และประเมินผลความเสี่ยง วิเคราะห์และประเมินเพื่อทราบช่องว่างหรือช่องโหว่ (Gap)

6. กำหนดแนวทางแก้ไขความเสี่ยงเพื่อปิดช่องโหว่

7. เลือกใช้มาตรการความความมั่นคงปลอดภัยที่เหมาะสม และควบคุมตามมาตรฐาน เพื่อจัดการความเสี่ยง

8. นำมาตรการความมั่นคงปลอดภัยที่เลือกไปปฏิบัติ โดยการจัดทำเอกสารขั้นตอนการปฏิบัติงานมาตรฐาน/แนวทางการปฏิบัติงาน กำหนดแบบฟอร์มต่าง ๆ ที่จำเป็น และฝึกอบรมพนักงานเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุก ๆ ระดับ

9. ตรวจประเมินภายในระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ

10. ทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร ทบทวนประเมินความเสี่ยง ระดับความเสี่ยงที่ยอมรับได้ และความเสี่ยงที่ยังเหลืออยู่

11. จัดให้มีวิธีตรวจสอบ วัดผล ทบทวน และประเมินผลระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ ซึ่งจะทำให้การบริหารความมั่นคงปลอดภัยของสารสนเทศมีประสิทธิภาพและต่อเนื่อง

12. ปรับปรุงระบบบริหารความมั่นคงปลอดภัยของสารสนเทศตามสิ่งที่ตรวจพบ วิเคราะห์หาสาเหตุของปัญหาที่แท้จริง ดำเนินการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก และจัดให้มีระบบการจัดการเอกสารและบันทึกสิ่งที่เกิดขึ้นจากการจัดทำระบบบริหารความมั่งคงปลอดภัยของสารสนเทศ

ผู้ประเมินคุณภาพภายในระดับมหาวิทยาลัย ปี 2550

มหาวิทยาลัยมีคำสั่งแต่งตั้งคณะกรรมการประเมินคุณภาพการศึกษาภายในระดับมหาวิทยาลัย รอบปีการศึกษา 2549 ดังนี้

1. อาจารย์ปรานี พรรณวิเชียร ประธานกรรมการ
2. รศ.ดร.ชนศักดิ์ บ่ายเที่ยง กรรมการ
3. ผศ.อัจฉรา สังข์สุวรรณ กรรมการ
4. รศ.ดร.วิบูลย์ ชื่นแขก กรรมการ
5. รศ.ดร.พานิช วุฒิพฤกษ์ กรรมการ
6. นางศิริวิช ดโนทัย กรรมการ
7. นายเทวินทร์ จันทรศักดิ์ กรรมการและเลขานุการ
8. นายปิยะชาติ โชคพิพัฒน์ กรรมการและผู้ช่วยเลขานุการ
9. นางสาวอรทัย แสงธำรง กรรมการและผู้ช่วยเลขานุการ
10. นางสาวอรสา ศิริราช กรรมการและผู้ช่วยเลขานุการ