บทที่ 5

สรุปผลการศึกษาและข้อเสนอแนะ

สรุปผลการวิจัย

จากการศึกษาวิจัย เรื่อง การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศในอุตสาหกรรมวิทยุโทรทัศน์โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้ และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีศึกษาองค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย (ThaiPBS)

โดยการศึกษาจะเริ่มจากสำรวจการดำเนินงานตามมาตรฐาน ISO/IEC 27001 ในปัจจุบันโดยการสัมภาษณ์เชิงนโยบาย จากนั้นทำการสำรวจความคิดเห็นของกลุ่มตัวอย่างที่มีต่อการดำเนินงานทางสารสนเทศภายในองค์การ และสุดท้ายทำการวิเคราะห์ความเสี่ยงที่เกิดขึ้นภายในองค์การ เพื่อนำผลการสำรวจที่ได้จาก 3 ส่วนมาทำการวางมาตรการเพื่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศภายในองค์การ โดยทั้งนี้การวางมาตรการต้องให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วย

ตารางที่ 5.1

สรุปผลการสำรวจ การปฏิบัติงานตามกรอบ ISO/IEC 27001 ขององค์การฯ ในปัจจุบัน

สถานการณ์ดำเนินงานตามกรอบ ISO/IEC27001	หมวด ISO/IEC27001	คิดเป็นร้อยละ
ยังไม่เริ่มดำเนินการ	หมวดที่ 1 : 1.1.1, 1.1.2 หมวดที่ 2 : 2.1.1, 2.1.2, 2.1.3, 2.1.5, 2.1.6, 2.1.7, 2.2.1, 2.2.2, 2.2.3 หมวดที่ 3 : - หมวดที่ 4 : 4.2.1, 4.2.3, 4.3.1, 4.3.3 หมวดที่ 5 : - หมวดที่ 6 : 6.1.1, 6.1.2, 6.5.1, 6.6.1, 6.6.2, 6.7.2, 6.7.4, 6.8.1, 6.8.2, 6.8.3, 6.8.5, 6.9.1,	55.63

สถานการณ์ดำเนินงานตามกรอบ ISO/IEC27001	หมวด ISO/IEC27001	คิดเป็นร้อยละ
ยังไม่เริ่มดำเนินการ	6.9.2, 6.9.3, 6.10.1, 6.10.2, 6.10.3, 6.10.4, 6.10.5 หมวดที่ 7 : 7.1.1, 7.2.3, 7.2.4, 7.3.1, 7.3.2, 7.3.3, 7.4.1, 7.4.7, 7.5.3, 7.5.5, 7.5.6, 7.6.2, 7.7.2 หมวดที่ 8 : 8.1.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.3.1, 8.3.2, 8.4.1, 8.5.1, 8.5.4, 8.6.1 หมวดที่ 9 : 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3 หมวดที่ 10 : 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5 หมวดที่ 11 : 11.1.3,11.1.4, 11.1.5, 11.1.6, 11.2.1, 11.2.2	55.63
กำลังดำเนินการ	หมวดที่ 1 : - หมวดที่ 2 : 2.1.8 หมวดที่ 3 : - หมวดที่ 4 : 4.1.1, 4.2.2 หมวดที่ 5 : - หมวดที่ 6 : 6.7.1, 6.7.3, 6.8.4 หมวดที่ 7 : 7.2.1, 7.2.2, 7.5.1, 7.5.4, 7.7.1, หมวดที่ 8 : - หมวดที่ 9 : - หมวดที่ 10 : - หมวดที่ 11 : 11.1.1, 11.3.1, 11.3.2	10.53
ดำเนินการแล้วเสร็จ	หมวดที่ 1 : - หมวดที่ 2 : 2.1.4 หมวดที่ 3 : 3.1.1, 3.1.2, 3.1.3, 3.2.1, 3.2.2 หมวดที่ 4 : 4.1.2, 4.1.3, 4.3.2 หมวดที่ 5 : 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6,	33.84

สถานการณ์ดำเนินงานตามกรอบ ISO/IEC27001	หมวด ISO/IEC27001	คิดเป็นร้อยละ
ดำเนินการแล้วเสร็จ	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 หมวดที่ 6 : 6.1.3, 6.1.4, 6.2.1, 6.2.2, 6.2.3, 6.3.1, 6.3.2, 6.4.1, 6.4.2, 6.10.6 หมวดที่ 7 : 7.4.2, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.5.2, 7.6.1 หมวดที่ 8 : 8.4.2, 8.4.3, 8.5.2, 8.5.3, 8.5.5 หมวดที่ 9 : - หมวดที่ 10 : - หมวดที่ 11 : 11.1.2	55.63

จากผลการสำรวจการปฏิบัติงานตามกรอบ ISO/IEC 27001 ขององค์การฯ ในปัจจุบันจะสรุปผลได้ดังนี้ ถ้าองค์การฯ ต้องการที่ก้าวไปสู่การรับรองการดำเนินงานทางด้านสารสนเทศตามกรอบ ISO/IEC27001 องค์การฯ จึงควรให้ความสนใจและปฏิบัติตามในส่วนของหมวดที่ยังไม่ได้ดำเนินงานซึ่งมีเปอร์เซ็นต์มากถึง 55.63 % และต้องดำเนินการตรวจสอบในหมวดที่กำลังดำเนินการอยู่ที่มีอยู่ 10.53 % ว่าถูกต้องครบถ้วนตาม ISO/IEC27001 หรือไม่

ตารางที่ 5.2
สรุปผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ที่มีต่อการดำเนินงานตามกรอบ ISO/IEC 27001 ขององค์การในปัจจุบัน

มาตรฐาน ISO/IEC 27001	ผลการสำรวจระดับความเหมาะสม
หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	ส่วนใหญ่ไม่ทราบนโยบาย
หมวดที่ 2 ด้านโครงสร้างทางด้านความมั่งคงปลอดภัยภายในองค์การ (Internal Organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)	ระดับน้อย

มาตรฐาน ISO/IEC 27001	ผลการสำรวจระดับความเหมาะสม
หมวดที่ 3 ด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์การ (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)	ระดับมาก
หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	ระดับน้อยที่สุด
หมวดที่ 5 ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	ระดับสูงที่สุด
หมวดที่ 6 ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and Operations Management)	ระดับน้อย
หมวดที่ 7 ด้านการควบคุมการเข้าถึง (Access Control)	ระดับน้อย
หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance)	ระดับปานกลาง
หมวดที่ 9 ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การ (Information Security Incident Management)	ระดับน้อยที่สุด
หมวดที่ 10 ด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์การ (Business Continuity Management)	ระดับปานกลาง
หมวดที่ 11 ด้านการปฏิบัติตามข้อกำหนด (Compliance)	ระดับน้อย

ตารางที่ 5.3
ลำดับเหตุการณ์ความเสี่ยงทั้ง 3 ด้านทั้งหมดองค์การ
โดยเรียงลำดับจากระดับความเสี่ยงสูงไปหาความเสี่ยงน้อย

ลำดับ	เหตุการณ์ที่ก่อให้เกิด ความเสี่ยงภายในองค์การ	ระดับ ความเสี่ยง	ประเภท ความเสี่ยง
1	การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	78.45 สูง	Confidentiality
2	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่อง คอมพิวเตอร์ในองค์การได้	68.21 สูง	Integrity
3	การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง	63.36 สูง	Integrity
4	การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ	59.62 สูง	Integrity
5	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน	58.61 สูง	Confidentiality
6	การดูแลรักษา (Maintenance) ระบบ ทำให้ ระบบไม่สามารถใช้งานได้	54.54 สูง	Availability
7	การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ ถูกต้อง	51.78 สูง	Confidentiality
8	ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และ ซอฟต์แวร์ ทำงานผิดพลาด	51.49 สูง	Integrity
9	การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง	50.30 สูง	Confidentiality
10	ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ	50.71 สูง	Availability
11	การขาดการพัฒนา หรือปรับปรุงระบบรักษา ความปลอดภัยของข้อมูล	50.30 สูง	Integrity

ลำดับ	เหตุการณ์ที่ก่อให้เกิด ความเสี่ยงภายในองค์การ	ระดับ ความเสี่ยง	ประเภท ความเสี่ยง
12	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	49.97 สูง	Confidentiality
13	การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม	36.86 ปานกลาง	Confidentiality
14	การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง	33.18 ปานกลาง	Availability
15	มีการแก้ไขโปรแกรมประยุกต์ (Application) ไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ	30.09 ปานกลาง	Integrity
16	การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง	29.86 ปานกลาง	Confidentiality
17	ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย	28.60 ปานกลาง	Integrity
18	การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป	23.14 ปานกลาง	Availability
19	พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม	21.69 ปานกลาง	Availability
20	การเกิดความผิดพลาดในการรายงานผลข้อมูล	21.15 ปานกลาง	Integrity
21	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	15.72 ต่ำ	Availability
22	งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ	14.86 ต่ำ	Availability
23	ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย	14.14 ต่ำ	Availability
24	การเข้าใช้ข้อมูลสำคัญโดยปราศจากการควบคุม	12.34 ต่ำ	Confidentiality

ลำดับ	เหตุการณ์ที่ก่อให้เกิด ความเสี่ยงภายในองค์การ	ระดับ ความเสี่ยง	ประเภท ความเสี่ยง
25	กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ	7.20 ต่ำ	Integrity

มาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

จากผลการสำรวจทางด้านความเสี่ยง ผู้วิจัยจะสร้างมาตรการในการลดความเสี่ยงทั้ง 25 เหตุการณ์ โดยแบ่งเป็น 3 ระยะ ดังนี้ คือ

ระยะที่ 1 เป็นมาตรการลดความเสี่ยงสูงจำนวน 12 เหตุการณ์

ประกอบด้วย

ด้าน Availability 2 เหตุการณ์ Confidentiality 2 เหตุการณ์ Integrity 2 เหตุการณ์

ระยะที่ 2 เป็นมาตรการลดความเสี่ยงปานกลางจำนวน 8 เหตุการณ์

ประกอบด้วย

ด้าน Availability 2 เหตุการณ์ Confidentiality 2 เหตุการณ์ Integrity 2 เหตุการณ์

ระยะที่ 3 เป็นมาตรการลดความเสี่ยงต่ำจำนวน 5 เหตุการณ์

ประกอบด้วย

ด้าน Availability 2 เหตุการณ์ Confidentiality 2 เหตุการณ์ Integrity 2 เหตุการณ์

มาตรการในระยะที่ 1 : เป็นมาตรการลดความเสี่ยงสูงจำนวน 12 เหตุการณ์ดังนี้

1. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล
2. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้
3. การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง
4. การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ
5. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน
6. การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้
7. การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง
8. ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด

9. การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง
10. ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ
11. การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานให้ทันสมัย
12. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม

โดยวิธีที่องค์การจะใช้ในการลดความเสี่ยงในระยะที่ 1 คือการสร้างนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เป็นลายลักษณ์อักษร โดยใช้มาตรฐาน ISO/IEC 27001 เป็นแนวทาง และมีประกาศใช้อย่างเป็นทางการ

ตารางที่ 5.4 มาตรการในการลดความเสี่ยงในระดับสูง

เหตุการณ์ที่	ประเภทความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
1.	Confidentiality	1. องค์การไม่อนุญาตให้ใช้รหัสผ่านร่วมกัน และความยาวของรหัสผ่าน ต้องไม่น้อยกว่า 6 ตัวอักษร และต้องเปลี่ยนรหัสผ่านทุก 1 เดือน (พนักงานทั่วไป) 2. รหัสผ่านถือเป็นทรัพย์สินขององค์การ ไม่อนุญาตให้บอกรหัสผ่านแก่บุคคลอื่น (พนักงานทั่วไป)	หมวด 1 หมวด 4 พ.ร.บ. คอมพิวเตอร์
2.	Availability	องค์จะต้องมีการจัดให้มีชื่อผู้ใช้ และรหัสผ่านให้กับพนักงาน และกำหนดสิทธิ์ในการเข้าถึง (ฝ่าย IT)	หมวด 1 หมวด 7
3.	Integrity	ในการดำเนินการแก้ไขระบบทุกครั้ง จะต้องมีการบันทึกวันและเวลาที่ดำเนินการแก้ไข สาเหตุ วิธีการแก้ไข และรายชื่อผู้ดำเนินการแก้ไขไว้เป็นลายลักษณ์อักษรทุกครั้ง (ฝ่าย IT)	หมวด 6

เหตุการณ์ที่	ประเภทความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
4.	Integrity	1. หัวหน้า IT ต้องมีการกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยอย่างชัดเจน 2. องค์การต้องมีการตรวจสอบการบริหารจัดการจากผู้ตรวจสอบอิสระ	หมวด 1 หมวด 2
5.	Confidentiality	ต้องมีการจัดอบรมให้ความรู้ทางด้านเทคโนโลยีสารสนเทศ เดือนละ 1 ครั้ง (ฝ่าย IT)	หมวด 1 หมวด 4
6.	Availability	ในการดูแลรักษาระบบควรแจ้งให้ผู้ใช้งานทราบล่วงหน้า 3 วันทำการ (ฝ่าย IT)	หมวด 1 หมวด 8
7.	Confidentiality	ต้องมีการจัดอบรมให้ความรู้ทางด้านเทคโนโลยีสารสนเทศ เดือนละ 1 ครั้ง (ฝ่าย IT)	หมวด 4
8.	Integrity	มีการตรวจสอบระบบการใช้งานที่เป็นซอฟต์แวร์ทุก 1 อาทิตย์ และมีการตรวจสอบการใช้งานฮาร์ดแวร์ทุก 1 เดือน (ฝ่าย IT)	หมวด 6 หมวด 8
9.	Confidentiality	1. ต้องถอดสิทธิการใช้งานแก่ผู้ใช้งานทันทีที่พ้นสภาพการเป็นพนักงาน (ฝ่าย IT) 2. ควรมีการแจ้ง และสรุปสิทธิการใช้งานระบบต่างๆให้แก่ผู้ใช้งานทราบทุก 6 เดือน (ฝ่าย IT)	หมวด 4

เหตุการณ์ที่	ประเภท ความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
10.	Availability	ผู้ดูแลระบบฐานข้อมูลต้องสำรองข้อมูลทุกวัน และต้องทำการทดสอบข้อมูลทุก 1 เดือน (ฝ่าย IT)	หมวด 6
11.	Integrity	ต้องมีการอัพเดท ระบบป้องกันไวรัสให้ทันสมัยอยู่เสมอ	หมวด 1
12.	Confidentiality	1. มีการจำกัดสิทธิในการพิมพ์ 2. มีบทลงโทษสำหรับผู้เผยแพร่ข้อมูลขององค์กร	หมวด 2 หมวด 4 หมวด 7

สรุป นโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ จะถูกแบบเป็น 2 ส่วน คือ

ส่วนที่ 1 : สำหรับพนักงานทั่วไป สำหรับใช้เป็นแนวทางในการเข้าใช้ระบบสารสนเทศ เพื่อช่วยลดความเสี่ยงที่จะเกิดขึ้นกับองค์การ

ส่วนที่ 2 : สำหรับเจ้าหน้าที่สารสนเทศ สำหรับใช้เป็นแนวทางในการเพิ่มความมั่นคงปลอดภัยให้กับระบบสารสนเทศ

ส่วนที่ 1 นโยบายทางด้านความมั่นคงปลอดภัยของสารสนเทศ สำหรับพนักงานทั่วไป

1) องค์การ ไม่สนับสนุน หรือยินยอมให้พนักงานขององค์การ กระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง
   1.1) ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์การ หรือบุคคลอื่นๆ
   1.2) ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
   1.3) ห้ามส่งจดหมายอิเล็กทรอนิกส์หรือการสื่อสารทางอิเล็กทรอนิกส์ใดๆ โดยไม่ระบุชื่อผู้ส่ง (SPAM e-mail)

2) องค์การ จะจัดให้มีชื่อผู้ใช้ (USER ID) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับ อินเทอร์เน็ต เป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่าน ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม กฎการใช้รหัสผ่าน

   2.1) ความยาวของตัวอักษรต้องไม่น้อยกว่า 6 ตัวอักษร และห้ามเป็นชื่อ – นามสกุลของผู้ใช้งาน

   2.2) ผู้ใช้งานต้องมีการเปลี่ยน รหัสผ่าน (Password) ในการเข้าใช้ระบบทุก 1 เดือน และหากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน

3) องค์การ ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน

4) ไม่อนุญาตให้ใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์ประกอบอื่นที่มิใช้ขององค์การ ในการเชื่อมต่อเข้ากับเครือข่ายขององค์การ

5) ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็กทรอนิกส์ การสนทนาหรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายขององค์การ ได้แก่

   - การรักษาความลับของเอกสาร ห้ามส่งเอกสารความลับโดยจดหมายอิเล็กทรอนิกส์ยกเว้นได้รับการเข้ารหัสโดยได้รับการยืนยันจากหน่วยงานคอมพิวเตอร์

6) ไม่อนุญาตให้พนักงานใช้ e-mail อื่นใดที่องค์การ ไม่ได้กำหนดให้ใช้

7) ในกรณีการขอใช้อีเมล์ของรายการต่างๆ ขององค์การ ถ้าผู้ดูแลรายการมีความประสงค์ต้องการใช้ อีเมล์รายการโต้ตอบกับผู้ชม ผู้ดูแลรายการนั้นจะต้องเซ็นหนังสือยินยอมเป็นผู้รับผิดชอบของอีเมล์ของรายการนั้น และถ้าในกรณีที่ผู้ดูแลรายการเป็นบุคคลภายนอกจะต้องมีพนักงานขององค์การ เซ็นกำกับในหนังสือยินยอมเป็นผู้รับผิดชอบของอีเมล์ของรายการนั้นด้วย

8) การเข้าใช้งาน application ต่างๆ จะต้องได้รับอนุญาตจากเจ้าของระบบโดยให้ผู้บังคับบัญชาโดยตรงเป็นผู้ขอสิทธิในการใช้

9) ห้ามพนักงานนำ โปรแกรม หรือ Application ใดๆมาติดตั้งบนเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์รวมถึงอุปกรณ์ประกอบอื่นๆ องค์การ โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์และผู้บังคับบัญชาโดยตรง
10) ห้ามพนักงานใช้ โปรแกรม หรือ Application ที่ไม่ถูกลิขสิทธิ์
11) หากพบว่ามีการส่งข้อมูลที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือผิดต่อกฎระเบียบขององค์การฯ ให้แจ้งต่อผู้บังคับบัญชาโดยตรงหรือเจ้าหน้าที่หน่วยงานคอมพิวเตอร์
12) ถ้าพนักงานท่านได้ไม่ปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ พนักงานท่านนั้นต้องได้รับบทลงโทษ ตามผู้บังคับบัญชาเห็นสมควร

ส่วนที่ 2 นโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ สำหรับฝ่ายสารสนเทศ

เพื่อใช้เป็นแนวทางในการเข้าใช้ระบบสารสนเทศ เพื่อช่วยลดความเสี่ยง และเพิ่มความมั่นคงปลอดภัยให้กับระบบสารสนเทศภายในองค์การ มีรายละเอียดดังต่อไปนี้

1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจัดอบรมให้ความรู้ทางด้านเทคโนโลยีสารสนเทศรวมถึงปฏิบัติในการเข้าใช้ระบบสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย เดือนละ 1 ครั้ง
2) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการประชาสัมพันธ์ ให้กับผู้ใช้งานทราบถึงนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้ผู้ใช้งานเข้าใช้ และตระหนักถึงความสำคัญในการปฏิบัติ เพื่อความมั่นคงปลอดภัยของข้อมูล
3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการอัพเดท ระบบป้องกันไวรัสให้ทันสมัยอยู่เสมอ
4) ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการแจ้ง หรือสรุป สิทธิการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์การ ให้แก่ผู้ใช้งานทราบทุก 6 เดือน
5) ฝ่ายเทคโนโลยีสารสนเทศ ควรมีการถอดสิทธิการเข้าใช้งานแก่ผู้ใช้งานทันที ที่ผู้ใช้งานท่านนั้น พ้นสภาพการเป็นพนักงานขององค์การ

6) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดอบรมความรู้เกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้กับพนักงานทุกท่าน รวมถึงพนักงานที่เข้ามาใหม่ด้วย และมีการประสัมพันธ์ให้พนักงานทุกท่านตระหนักถึงความสำคัญของการปฏิบัติตามกฎหมาย

7) ในการบำรุงรักษาระบบ ควรกระทำ เมื่อที่ไม่มีการเรียกใช้งานจากผู้ใช้ หรือถ้าไม่สามารถกระทำได้ ควรจะแจ้งเป็นลายลักษณ์อักษรให้ผู้ใช้งานทราบล่วงหน้า 3 วันทำการ

8) ผู้ดูแลระบบฐานข้อมูล ต้องทำการสำรองข้อมูลของแต่ละระบบทุกวัน

9) ผู้ดูแลระบบฐานข้อมูล ต้องทำการทดสอบข้อมูลที่สำรองไว้ทุกๆ 1 เดือน เพื่อตรวจสอบว่าข้อมูลที่ได้สำรองครบถ้วน และสามารถนำกลับมาใช้ใหม่ได้

10) ในการดำเนินการแก้ไขระบบ จะต้องมีการบันทึกวันและเวลาที่ดำเนินการแก้ไข สาเหตุ วิธีการแก้ไข และรายชื่อผู้ดำเนินการแก้ไขไว้เป็นลายลักษณ์อักษรทุกครั้ง

มาตรการในระยะที่ 2 : เป็นมาตรการลดความเสี่ยงปานกลางจำนวน 8 เหตุการณ์ดังนี้

1. การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม

2. การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง

3. มีการแก้ไขโปรแกรมประยุกต์ (Application) อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ

4. การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง

5. ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย

6. การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป

7. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม

8. การเกิดความผิดพลาดในการรายงานผลข้อมูล

หลังจากที่วิธีที่องค์การฯ ได้จัดทำและประกาศใช้นโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เป็นลายลักษณ์อักษรเพื่อลดความเสี่ยงในระยะที่ 1 โดยแบ่งเป็น 2 ส่วน

แล้วนั้น ในระยะที่ 2 จะใช้วิธีการเพิ่มเติมแนวทางในการปฏิบัติจากนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศของเดิม โดยใช้มาตรฐาน ISO/IEC 27001 เป็นแนวทาง และมีประกาศใช้เพิ่มเติม

ตารางที่ 5.5 มาตรการในการลดความเสี่ยงในระดับปานกลาง

เหตุการณ์ที่	ประเภท ความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
1.	Confidentiality	1. รหัสผ่านถือเป็นทรัพย์สินขององค์การ ไม่อนุญาตให้บอกรหัสผ่านแก่บุคคลอื่น 2. ฝ่าย IT ต้องมีการอบรมให้ความรู้ แก่พนักงาน	หมวดที่ 4 พรบ. คอมพิวเตอร์
2.	Availability	1. ในการคัดเลือกคุณสมบัติของเจ้าหน้าที่ IT ควรมีการระบุประสบการณ์ความสามารถอย่างชัดเจน 2. มีการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ หรืออุปกรณ์ประมวลผล 3. จัดทำคู่มือการติดตั้ง และทบทวนให้เข้าใจก่อนการติดตั้งทุกครั้ง	หมวด 1 หมวด 4 หมวด 6
3.	Integrity	ต้องมีการควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ และต้องมีการบันทึกไว้เป็นลายลักษณ์อักษรทุกครั้ง(ฝ่าย IT)	หมวดที่ 6
4.	Confidentiality	มีกระบวนการตรวจสอบความถูกต้องขอข้อมูลอยู่เสมอ	หมวดที่ 8

เหตุการณ์ที่	ประเภท ความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
5.	Integrity	จัดทำนโยบายทางด้านความมั่นคงปลอดภัย (ฝ่าย IT)	หมวดที่ 1
6.	Availability	ก่อนการจัดหาและพัฒนา ควรมีการระบุขอบเขตชัดเจน และผ่านการวิเคราะห์จากผู้เชี่ยวชาญ เป็นลายลักษณ์อักษรก่อนทุกครั้ง และเมื่อจัดทำแล้วให้ทดสอบก่อนใช้งานจริงโดยผู้ใช้งานและในระบบขององค์การ	หมวด 8
7.	Availability	อบรมให้ความรู้ แก่พนักงาน (ฝ่าย IT)	หมวด 4
8.	Integrity	มีการตรวจสอบข้อมูล ตั้งแต่ ก่อน ระหว่าง และหลังการประมวลผล (ฝ่าย IT)	หมวดที่ 8

โดยนโยบายที่จะทำการประกาศใช้เพิ่มเติมจะเป็นนโยบายสำหรับเจ้าหน้าที่สารสนเทศเท่านั้น โดยสรุปสิ่งที่เพิ่มเติมดังนี้

11) จะต้องมีการจัดทำคู่มือในการติดตั้งฮาร์ดแวร์ หรือ ซอฟต์แวร์ ที่เป็นลายลักษณ์อักษร และต้องมีการปรับปรุงคู่มือให้ทันสมัยอยู่เสมอ และในการดำเนินงานต้องดำเนินโดยผู้เชี่ยวชาญเท่านั้น

12) เจ้าหน้าที่สารสนเทศ จะต้องมีการบันทึกผลการตรวจสอบข้อมูลตั้งแต่ ก่อน ระหว่าง และหลังการประมวลผล

13) หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ ต้องมีการกำหนดคุณสมบัติของเจ้าหน้าที่สารสนเทศ และดำเนินการทดสอบคุณสมบัติในการคัดเลือกพนักงาน ให้ตรงกับลักษณะงานที่ต้องการ

14) เจ้าหน้าที่สารสนเทศต้องได้รับการอบรม เกี่ยวกับความรู้ทางด้านความชำนาญตามสายงาน ปีละ 2 ครั้ง

มาตรการในระยะที่ 3 : เป็นมาตรการลดความเสี่ยงปานกลางจำนวน 5 เหตุการณ์ดังนี้

1. Router / Firewall เสียทำให้ไม่สามารถใช้งานได้
2. งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ
3. ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย
4. การเข้าใช้ข้อมูลสำคัญโดยปราศจากการควบคุม
5. กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ

สำหรับการลดความเสี่ยงในระยะที่ 3 จะใช้วิธีการเพิ่มมาตรการ เช่นเดียวกับในระยะที่ 2

ตารางที่ 5.6 มาตรการในการลดความเสี่ยงในระดับสูง

เหตุการณ์ที่	ประเภท ความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
1.	Availability	1. ผู้ที่ใช้เครือข่าย ต้องเป็นผู้ที่ได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น 2. ต้องมีการตรวจสอบการใช้งานอุปกรณ์ ทุก 1 เดือน	หมวด 1 หมวด 8
2.	Availability	1. ต้องมีการรายงานผลการดำเนินงานและให้ผู้บริหารเห็นความสำคัญของการสำรองข้อมูล 2. มีการวางแผนการใช้ทรัพยากรของระบบ ทุก 1 เดือน เพื่อทำการกำหนดงบประมาณไว้ล่วงหน้า	หมวด 1 หมวด 7

เหตุการณ์ที่	ประเภท ความเสี่ยง	มาตรการป้องกัน	ISO/IEC 27001
3.	Availability	มีการวางแผนการใช้ทรัพยากรของระบบ ทุก 1 เดือน (Capacity Management)	หมวด 6
4.	Confidentiality	มีการกำหนดสิทธิในการเข้าถึงข้อมูล และแยกความสำคัญของข้อมูลไว้เป็นประเภท	หมวด 1 หมวด 4 พ.ร.บ. คอมพิวเตอร์
5.	Integrity	มีการจัดอบรมการใช้งานแก่พนักงาน และเจ้าหน้าที่ทุก 1 เดือน	หมวดที่ 4

สรุปหัวข้อที่จะต้องเพิ่มเติมในนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยจะเพิ่มเติมในทั้ง 2 ส่วนของ นโยบายคือ

เพิ่มเติมในส่วนที่ 1 : สำหรับพนักงานทั่วไป มีรายละเอียดดังนี้ คือ

13) ผู้ที่ต้องการเข้าใช้ระบบเครือข่ายภายในองค์การฯ จะต้องกรอกแบบฟอร์มที่ทางฝ่ายเทคโนโลยีสารสนเทศจัดทำขึ้น และต้องได้รับการอนุมัติการผู้บังคับบัญชาเท่านั้น

เพิ่มเติมในส่วนที่ 2 : สำหรับเจ้าหน้าที่สารสนเทศ มีรายละเอียดดังนี้ คือ

15) ต้องมีการรายงานผลการปฏิบัติงาน สรุปปัญหา และผลกระทบของปัญหาที่เกิดขึ้นให้กับผู้บังคับบัญชา ทราบทุก 1 เดือน

16) เจ้าหน้าที่สารสนเทศต้องมีการตรวจการใช้งานอุปกรณ์ทางด้านระบบเครือข่ายทุก 1 เดือน

17) ต้องมีการวางแผนและตรวจสอบการใช้ทรัพยากรของระบบ ทุก 1 เดือน (Capacity Management)

ข้อเสนอแนะงานวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยมีข้อเสนอแนะเพื่อประโยชน์ต่อผู้จัดทำการวิจัยต่อจากงานวิจัยนี้ หรืองานวิจัยเรื่องอื่นๆ ที่มีส่วนสัมพันธ์กับงานวิจัยนี้ คือ

ข้อเสนอแนะสำหรับผู้วิจัย

1. ในการจัดทำแบบประเมิน และแบบสอบถามสำหรับสำรวจความคิดเห็น ต้องเข้าใจว่าพนักงานมีองค์ความรู้ และความเข้าใจแต่ละเรื่องที่แตกต่างกัน ดังนั้นต้องทำความเข้าใจพร้อมทั้งอธิบายความหมายของคำถามให้ชัดเจนก่อน หรือปรับปรุงคำถามให้ง่ายต่อความเข้าใจ เพื่อให้ได้ผลจากการตอบแบบสอบถามเป็นผลที่สามารถนำไปวิเคราะห์ได้จริง และเพื่อเวลานำมาตรฐานกลับมาประยุกต์ใช้ ได้จัดความเข้มข้นในการใส่ใจกับแต่ละกลุ่มตัวอย่างที่เหมาะสม ซึ่งเป็นการเตรียมความพร้อมและแก้ไขให้ตรงจุดและลดระยะเวลาในการดำเนินการ

2. ควรเพิ่มขอบเขตวิจัย โดยการขยายกลุ่มตัวอย่างให้ครอบคลุมมากยิ่งขึ้น โดยอาจนำกรณีศึกษาของบริษัทอื่นๆ ในอุตสาหกรรมเดียวกัน หรือในอุตสาหกรรมอื่นๆ ว่ามีความเสี่ยงที่คล้ายกัน เพื่อตั้งเป็นมาตรฐานในการนำไปกำหนดเป็นนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

สำหรับบริษัทอื่นๆ อุตสาหกรรมเดียวกับเรา ถ้ามีเหตุการณ์ความเสี่ยงเหตุการณ์ไหน ที่เป็นความเสี่ยงสูง เราจะได้นำมาเป็นแนวทางในการป้องกัน หรือปรับปรุงกระบวนการให้ดีขึ้น

3. ในการกำหนดเหตุการณ์ของความเสี่ยง ควรจะขึ้นอยู่กับสภาพแวดล้อม หรือให้ตรงกับวัตถุประสงค์การดำเนินงานในแต่ละบริษัท เพื่อให้นโยบายทางด้านความมั่นคงปลอดภัยที่จัดทำขึ้นสามารถนำมาลดความเสี่ยงที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะสำหรับองค์การ

1. องค์การควรนำมาตรการในการลดความเสี่ยงทั้ง 3 มาตรการประกาศเป็นนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารเทศ โดยแบ่งการประกาศใช้เป็น 3 ระยะ และถ้าต้องการให้นโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ที่ได้จัดทำขึ้นมานั้นสามารถนำมาลดความเสี่ยงให้ได้ผลดียิ่งขึ้น จำเป็นอย่างยิ่งที่ต้องได้รับการผลักดัน และการสนับสนุนจากผู้บริหาร

2. ในการนำมาตรฐานสากลมาใช้ บุคลากรจำเป็นที่จะต้องมีพร้อมทั้งทฤษฎี และนำไปประยุกต์ ดังนั้นองค์การจึงควรให้ความสำคัญในการอบรมความรู้เกี่ยวกับมาตรฐานสากลต่างๆ ให้กับบุคลากร เพื่อให้สามารถนำมาตรฐานต่างๆ มาประยุกต์ใช้อย่างมีประสิทธิภาพ

3. การนำนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศไปใช้ องค์กรควรมีการประเมินความเสี่ยง และทบทวนนโยบายอยู่อย่างสม่ำเสมอ เนื่องจากการเปลี่ยนแปลงทางเทคโนโลยีมีการเปลี่ยนแปลงอยู่เสมอ