บทที่ 4

ผลการวิจัย

ผลการวิเคราะห์เชิงพรรณนา

ข้อมูลที่จะนำมาวิเคราะห์ผลในงานวิจัยนี้ จะแบ่งออกเป็น 2 ส่วน คือ

ส่วนที่ 1 จะเป็นข้อมูลที่ได้จากการสัมภาษณ์ในการเชิงนโยบาย เพื่อตรวจสอบองค์การในปัจจุบันว่ามีการดำเนินงานตามกรอบมาตรฐาน ISO/IEC27001 ได้ครบถ้วนทั้ง 11 หมวดหรือไม่ ซึ่งผู้วิจัยจะใช้แบบประเมินองค์การตาม ISO/IEC27001 เป็นแนวทางในการสัมภาษณ์ โดยกลุ่มที่จะทำให้ข้อมูลในส่วนนี้คือ กลุ่มคณะผู้บริหาร หัวหน้าฝ่ายบริหารทรัพยากรบุคคล หัวหน้าฝ่ายบริหารงานทั่วไป และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ส่วนที่ 2 จะเป็นข้อมูลที่ได้จากการแบบสอบถาม โดยกำหนดขนาดของตัวอย่าง (ลูกค้า) โดยประมาณจากค่าสัดส่วนของประชากร (Proportions sample size determination) คำนวณจากสูตรของ *Taro Yamane* ที่คำนวณจากจำนวนพนักงานขององค์การกระจายเสียงแห่งประเทศไทยทั้งหมด 750 คน ผลการคำนวณได้จำนวนกลุ่มตัวอย่างทั้งหมด 261 คน แต่ในการแจกแบบสอบถามจริงผู้วิจัยได้แจกไปทั้งหมด 300 ชุด เพื่อป้องกันการสูญหาย และการสูญเสียของข้อมูล ผลปรากฏว่าได้ผู้ตอบแบบสอบถามมากลับมาทั้งสิ้น 285 คน

1. ผลการสำรวจลักษณะประชากรกลุ่มตัวอย่าง

เป็นข้อมูลทั่วไปของผู้ตอบแบบสอบถามทั้งหมด 285 คน สามารถจำแนกได้ดังนี้

- คิดเป็นเพศชาย เท่ากับ 54.74% และเพศหญิง เท่ากับ 45.26 % ดังแสดงในตาราง 4.1 และภาพ 4.1
- อายุน้อยกว่า 20 ปี เท่ากับ 0% , 21 - 25 ปี เท่ากับ 7.37 % , 26 – 30 ปี เท่ากับ 20.35 % , 31 – 35 ปี เท่ากับ 27.37 % . 36 – 40 ปี เท่ากับ 22.81 , 41 – 45 ปี เท่ากับ 14.04 % , 46 – 50 ปี เท่ากับ 5.61 % , 51 – 55 ปี เท่ากับ 1.75 % , มากกว่า 56 ปี เท่ากับ 0.70 % ดังแสดงในตาราง 4.2 และภาพ 4.2
- วุฒิการศึกษา ต่ำกว่าปริญญาตรี เท่ากับ 2.46 % , ปริญญาตรี เท่ากับ 78.25 % , ปริญญาโท เท่ากับ 18.25 % , ปริญญาเอก เท่ากับ 0.35 % ดังแสดงในตาราง 4.3 และภาพ 4.3

- ประสบการณ์ทำงานน้อยกว่า 1 ปี เท่ากับ 7.37 % , 1 – 2 ปี เท่ากับ 8.77 % , 3 – 4 ปี เท่ากับ 15.09 % , 5 – 10 ปี เท่ากับ 37.89 % , มากกว่า 10 ปี เท่ากับ 30.88 % ดังแสดงในตาราง 4.4 และภาพ 4.4
- ประสบการณ์ทำงานในองค์การในปัจจุบันน้อยกว่า 1 เดือน เท่ากับ 3.16 % , 1 – 4 เดือน เท่ากับ 5.61 % , 5 – 8 เดือน เท่ากับ 10.88 % , 9 -12 เดือน เท่ากับ 25.61 % , มากกว่า 1 ปี เท่ากับ 54.74 %
- แบ่งตามตำแหน่งงานเป็น ระดับปฏิบัติการ เท่ากับ 82.81 %

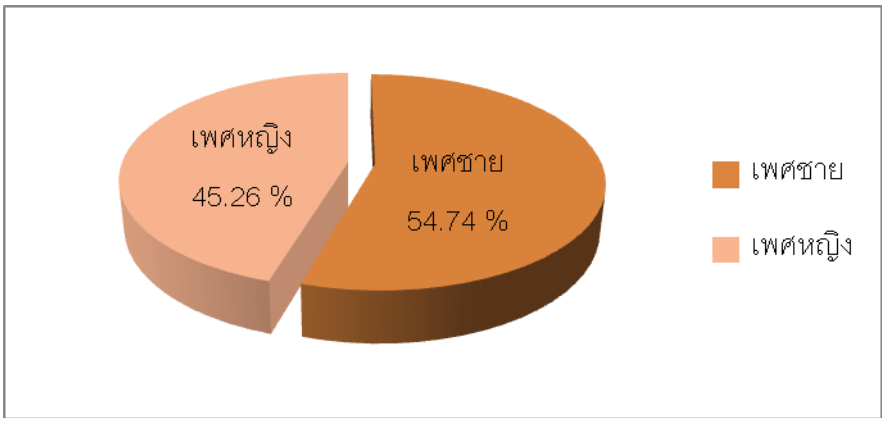
ตารางที่ 4.1

ร้อยละของกลุ่มตัวอย่าง จำแนกตามเพศของผู้ตอบแบบสอบถาม

เพศ	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
เพศชาย	156	54.74
เพศหญิง	129	45.26
จำนวนรวม	285	100

ภาพที่ 4.1

กราฟร้อยละของกลุ่มตัวอย่าง จำแนกตามเพศของผู้ตอบแบบสอบถาม



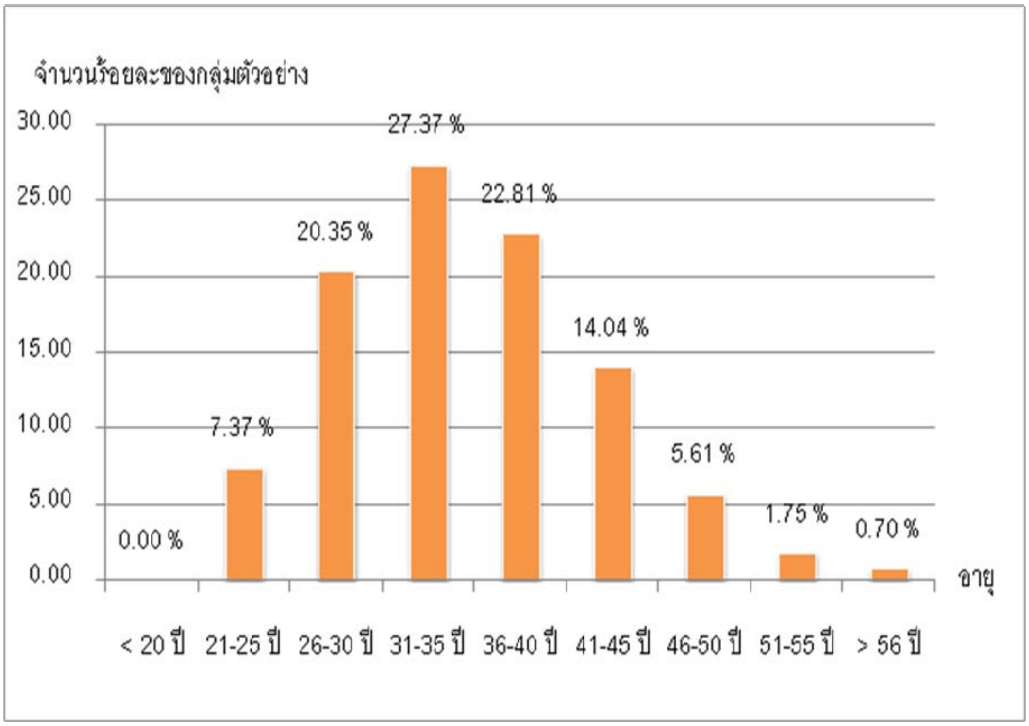
ตารางที่ 4.2

ร้อยละของกลุ่มตัวอย่าง จำแนกตามอายุของผู้ตอบแบบสอบถาม

อายุ	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
< 20 ปี	0	0.00
21-25	21	7.37
26-30	58	20.35
31-35	78	27.37
36-40	65	22.81
41-45	40	14.04
46-50	16	5.61
51-55	5	1.75
> 56	2	0.70
จำนวนรวม	285	100

ภาพที่ 4.2

ร้อยละของกลุ่มตัวอย่าง จำแนกตามอายุของผู้ตอบแบบสอบถาม



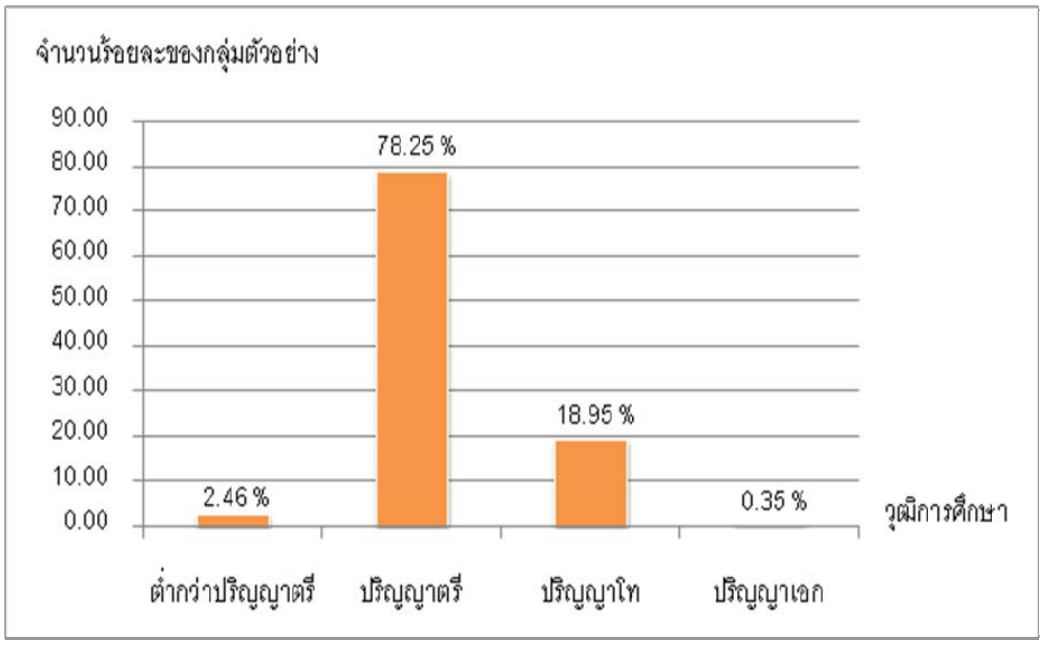
ตารางที่ 4.3

ร้อยละของกลุ่มตัวอย่าง จำแนกตามวุฒิการศึกษาของผู้ตอบแบบสอบถาม

วุฒิการศึกษา	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
ต่ำกว่าปริญญาตรี	7	2.46
ปริญญาตรี	223	78.25
ปริญญาโท	54	18.95
ปริญญาเอก	1	0.35
จำนวนรวม	285	100

ภาพที่ 4.3

ร้อยละของกลุ่มตัวอย่าง จำแนกตามวุฒิการศึกษาของผู้ตอบแบบสอบถาม



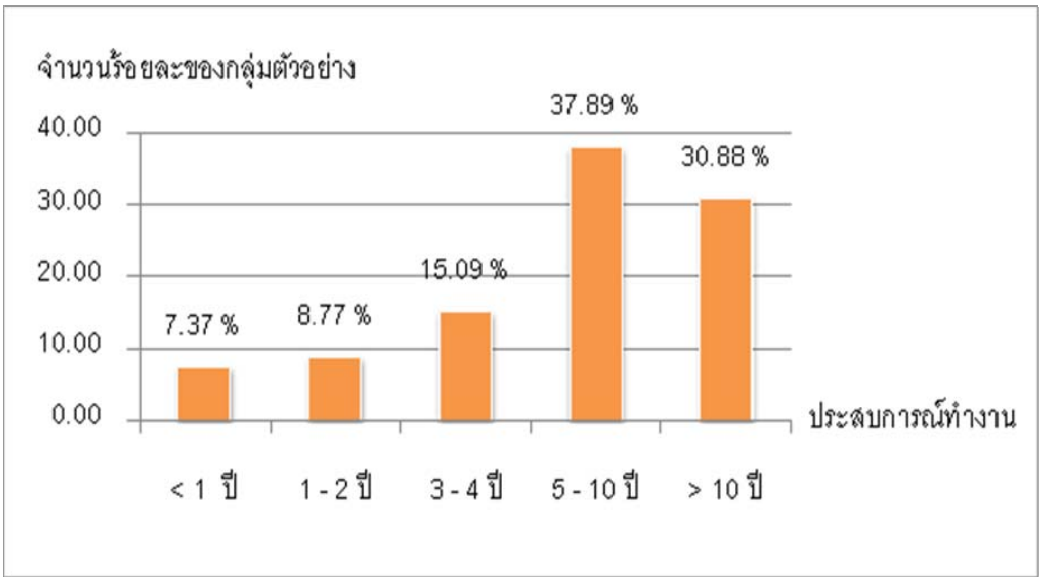
ตารางที่ 4.4

ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานของผู้ตอบแบบสอบถาม

ประสบการณ์ทำงาน	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
< 1 ปี	21	7.37
1 - 2 ปี	25	8.77
3 - 4 ปี	43	15.09
5 - 10 ปี	108	37.89
> 10 ปี	88	30.88
จำนวนรวม	285	100

ภาพที่ 4.4

ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานของผู้ตอบแบบสอบถาม



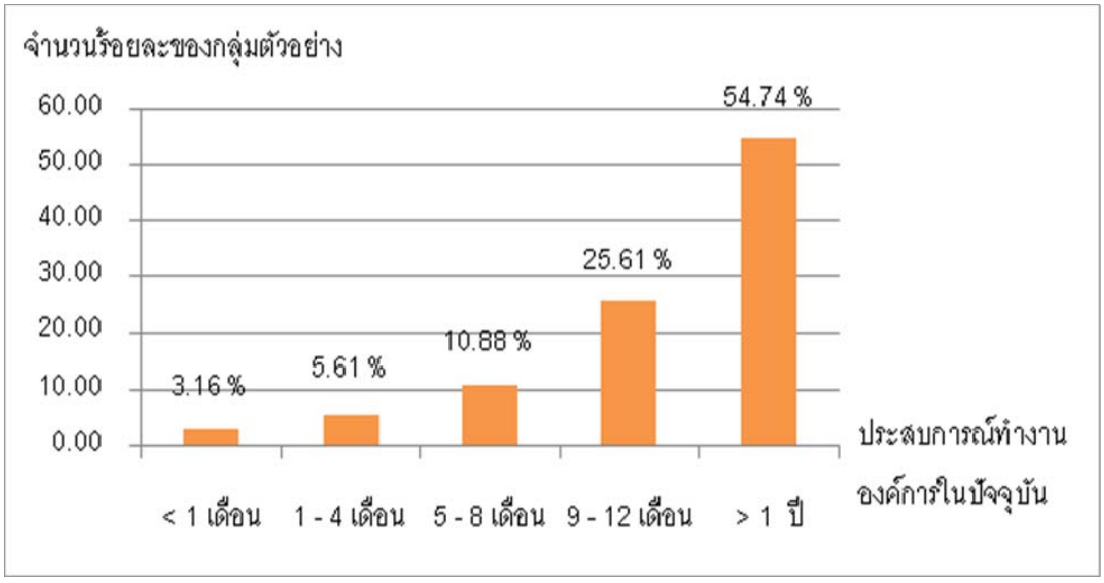
ตารางที่ 4.5

ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานองค์การในปัจจุบัน ของผู้ตอบแบบสอบถาม

ประสบการณ์ทำงานองค์การในปัจจุบัน	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
< 1 เดือน	9	3.16
1 - 4 เดือน	16	5.61
5 - 8 เดือน	31	10.88
9 - 12 เดือน	73	25.61
> 1 ปี	156	54.74
จำนวนรวม	285	100

ภาพที่ 4.5

ร้อยละของกลุ่มตัวอย่าง จำแนกตามประสบการณ์ทำงานองค์การในปัจจุบัน ของผู้ตอบแบบสอบถาม



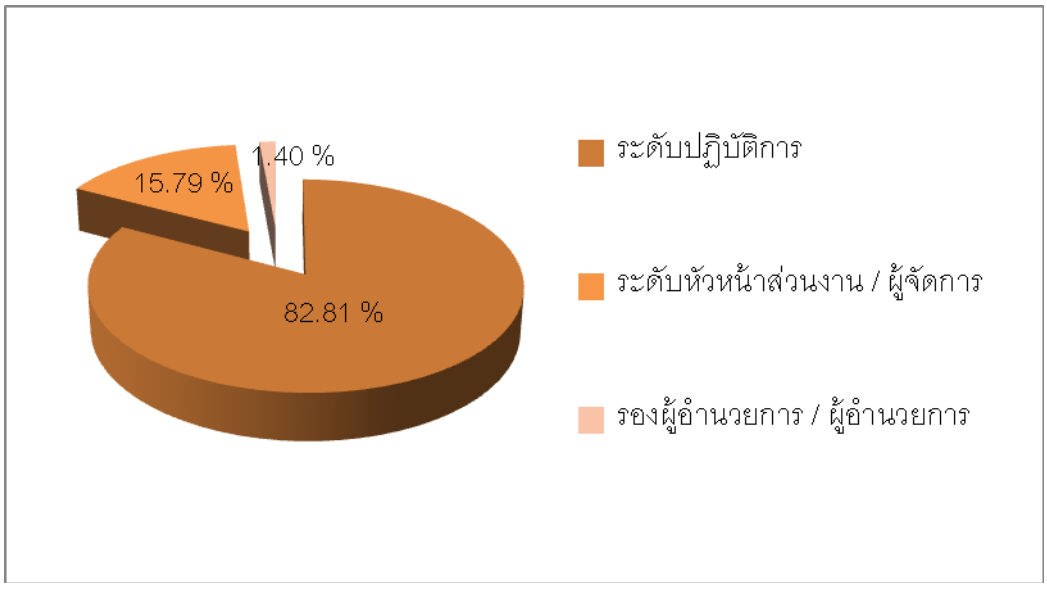
ตารางที่ 4.6

ร้อยละของกลุ่มตัวอย่าง จำแนกตามตำแหน่งงานในองค์การของผู้ตอบแบบสอบถาม

ประสบการณ์ทำงานองค์การในปัจจุบัน	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
ระดับปฏิบัติการ	236	82.81
ระดับหัวหน้าส่วนงาน / ผู้จัดการ	45	15.79
รองผู้อำนวยการ / ผู้อำนวยการ	4	1.40
จำนวนรวม	285	100

ภาพที่ 4.6

ร้อยละของกลุ่มตัวอย่าง จำแนกตามตำแหน่งงานในองค์การของผู้ตอบแบบสอบถาม



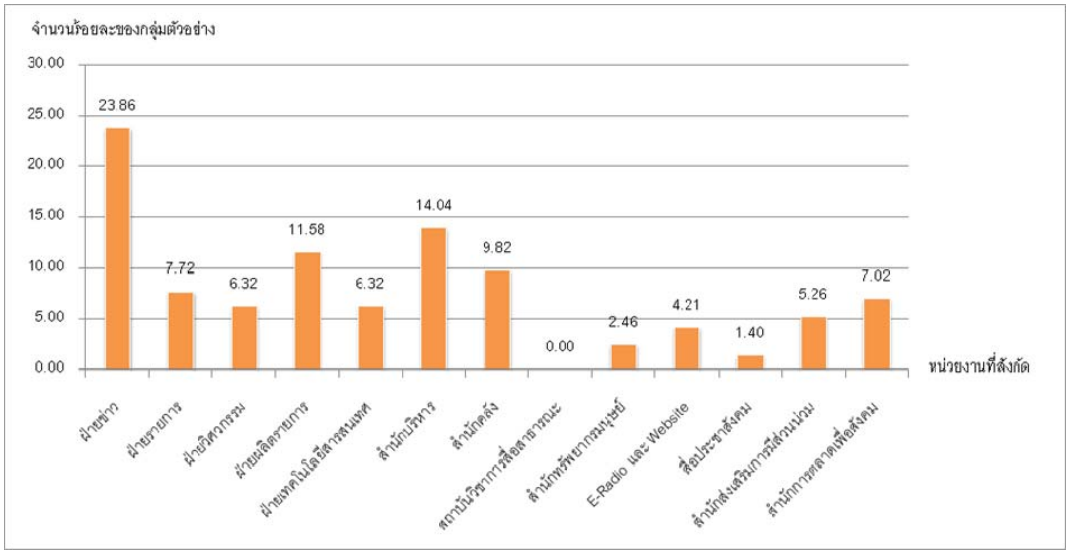
ตารางที่ 4.7

ร้อยละของกลุ่มตัวอย่าง จำแนกตามหน่วยงานที่สังกัดของผู้ตอบแบบสอบถาม

หน่วยงานที่สังกัด	จำนวนกลุ่มตัวอย่าง ในการตอบแบบสอบถาม	
	จำนวน	คิดเป็นร้อยละ
ฝ่ายข่าว	68	23.86
ฝ่ายรายการ	22	7.72
ฝ่ายวิศวกรรม	18	6.32
ฝ่ายผลิตรายการ	33	11.58
ฝ่ายเทคโนโลยีสารสนเทศ	18	6.32
สำนักบริหาร	40	14.04
สำนักคลัง	28	9.82
สถาบันวิชาการสื่อสาธารณะ	0	0.00
สำนักทรัพยากรมนุษย์	7	2.46
E-Radio และ Website	12	4.21
สื่อประชาสังคม	4	1.40
สำนักส่งเสริมการมีส่วนร่วม	15	5.26
สำนักการตลาดเพื่อสังคม	20	7.02
จำนวนรวม	285	100

ภาพที่ 4.7

ร้อยละของกลุ่มตัวอย่าง จำแนกตามหน่วยงานที่สังกัดของผู้ตอบแบบสอบถาม



2. ผลการสำรวจการดำเนินงาน ตามกรอบมาตรฐาน ISO/IEC27001

เป็นข้อมูลที่ได้จากการสัมภาษณ์เชิงนโยบาย โดยใช้แบบประเมินองค์การตามกรอบ ISO/IEC 27001 ทั้ง 11 หมวด เพื่อสำรวจการดำเนินงานทางด้านสารสนเทศ โดยมีผู้ตอบแบบสัมภาษณ์ คือ กลุ่มผู้บริหารองค์การฯ หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และหัวหน้าฝ่ายบริหารทรัพยากรมนุษย์

หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัย (Security Policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางองค์การ ฯ ยังไม่มีการจัดทำนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากองค์การฯ ไม่มีการจัดทำนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร ดังนั้นจึงยังไม่มีการทบทวนนโยบายความมั่นคงปลอดภัย

ตารางที่ 4.8

ผลการสำรวจ

หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัย (Security Policy)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)			
1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	✔		
1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	✔		

หมวดที่ 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)

2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)

ผู้ให้สัมภาษณ์ : กลุ่มผู้บริหารองค์การฯ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดทิศทาง คำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง และวิธีการมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์การฯ เพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์การ ฯ รวมถึงบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์การฯ ไว้เป็นลายลักษณ์อักษร

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้แล้ว เช่น มีการกรอก

แบบฟอร์มขอใช้เครื่องคอมพิวเตอร์ ที่ต้องการผ่านการอนุมัติโดยหัวหน้างาน ก่อนส่งมายังฝ่ายเทคโนโลยีสารสนเทศ จากนั้นหัวหน้าฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้อนุมัติให้ดำเนินการในการจัดหาและใช้งานอุปกรณ์ดังกล่าว

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน ทางองค์ยังไม่มีการจัดทำเอกสาร เพื่อให้มีการลงนามเป็นข้อตกลงระหว่างพนักงานกับองค์การฯ ว่าจะไม่เปิดเผยความลับขององค์การ ฯ

2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : สำหรับรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ. กสท โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น ในปัจจุบันองค์การฯ เองยังไม่มีการจัดทำเป็นเอกสารรวบรวมไว้ในที่เดียวกัน และเผยแพร่ให้เจ้าหน้าที่ทราบ จะมีเฉพาะเบอร์และชื่อผู้ติดต่อในหน่วยงานที่เคยติดต่อเท่านั้น ซึ่งอาจจะไม่ครบถ้วนสำหรับการดำเนินงานทางด้านความมั่นคงปลอดภัย และจะทราบเฉพาะอยู่ในกลุ่มเจ้าหน้าที่ที่เคยติดต่อเท่านั้นด้วย

2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

ผู้ให้สัมภาษณ์ : กลุ่มผู้บริหารองค์การฯ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ไม่มีชื่อ และเบอร์ผู้ติดต่อสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศหรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วมที่เป็นลายลักษณ์อักษร และไม่มีการรวมรวบไว้ในที่เดียวกัน

2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน องค์การฯ อยู่ระหว่างการถูกดำเนินการในการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ไม่มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และไม่มีการกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้อง กับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ไม่มีการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์การฯ เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์การฯ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ไม่มีการระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์การ ฯ และหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์การฯ

ตารางที่ 4.9

ผลการสำรวจ

หมวดที่ 2 : โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร

(Organization of information security)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)			
2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	✔		
2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	✔		
2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	✔		
2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)			✔
2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)	✔		
2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)	✔		
2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)	✔		
2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)		✔	

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)			
2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)	✔		
2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)	✔		
2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)	✔		

หมวดที่ 3 ด้านการบริหารจัดการทรัพย์สินขององค์กร (Asset management)

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)

3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายพัสดุ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการจัดทำ และ ปรับปรุงแก้ไขบัญชีทรัพย์สิน ที่เป็นลายลักษณ์อักษร

3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายพัสดุ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการเก็บข้อมูลเพื่อระบุความเป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ ตามที่กำหนดไว้ในบัญชีทรัพย์สิน

3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายพัสดุ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น

3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)

3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์การฯ ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

3.2.2 การจัดทำป้ายชื่อ และจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ มีการจัดทำป้ายชื่อ ที่ระบุความเป็นเจ้าของ ตามหมวดหมู่ของทรัพย์สินสารสนเทศที่ได้ตั้งไว้แล้ว

ตารางที่ 4.10

ผลการสำรวจ

หมวดที่ 3 ด้านการบริหารจัดการทรัพย์สินขององค์กร (Asset management)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)			
3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)			✔
3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)			✔
3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)			✔

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)			
3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)			✔
3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)			✔

หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศกำลังจัดทำเอกสารเพื่อกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงาน ผู้ที่องค์การฯ ทำสัญญาว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ มีการกำหนดคุณสมบัติตามลักษณะโดยตรง และดำเนินการตรวจสอบคุณสมบัติของผู้สมัคร ร่วมกับฝ่ายบริหารทรัพยากรมนุษย์ อย่างละเอียด

4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับงานทางด้านสารสนเทศ ดังนั้นจึงยังไม่มีการกำหนดเงื่อนไขการจ้างงานอย่างเป็นลายลักษณ์อักษร เพื่อให้ผู้ที่ได้รับการจ้างงานลงนามในการจ้างงานนั้นด้วย

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)

4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)

ผู้ให้สัมภาษณ์ : กลุ่มผู้บริหารองค์การฯ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากองค์การฯ ยังไม่มีการจัดทำนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กรที่เป็นลายลักษณ์อักษร ดังนั้น จึงยังไม่มีขั้นตอนและนโยบายเพื่อให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตาม

4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสนเทศได้มีการจัดอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ รวมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์การฯ โดยให้ฝ่ายบริหารทรัพยากรมนุษย์ ระบุเป็นหลักสูตรที่ผ่านการอบรมไว้ที่ประวัติของพนักงานด้วย

4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากองค์การฯ ยังไม่มีกำหนดนโยบายทางด้านความมั่นคงปลอดภัย และประกาศใช้อย่างเป็นทางการ จึงยังไม่มีการระบุถึงกระบวนการลงโทษ สำหรับผู้ที่กระทำผิด

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)

4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบันฝ่ายบริหารทรัพยากรมนุษย์ ยังไม่มีการกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่เลิกการจ้างงาน หรือ เป็นพนักงานที่เปลี่ยนลักษณะการจ้างงาน

4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรมนุษย์ และหัวหน้าฝ่ายพัสดุ

ข้อมูลที่ได้จากการสัมภาษณ์ : พนักงานขององค์การฯ ที่สิ้นสุดการจ้างงาน พนักงานต้องคืนทรัพย์สินทันที ตามรายชื่อความเป็นเจ้าตามที่ระบุไว้ในบัญชีทรัพย์สิน

4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เมื่อพนักงานขององค์การฯ สิ้นสุดการจ้างงาน ยังไม่มีการส่งข้อมูลที่เป็นลายลักษณ์อักษร การแจ้งของถอดสิทธิในการเข้าถึงระบบสารสนเทศ มายังฝ่ายเทคโนโลยีสารสนเทศ ทำให้พนักงานที่สิ้นสุดการจ้างงานไปแล้ว ยังคงมีสิทธิในการเข้าถึงระบบสารสนเทศภายในองค์การฯ

ตารางที่ 4.11

ผลการสำรวจ

หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)			
4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)		✔	
4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)			✔
4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)			✔
4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)			
4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)	✔		
4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)		✔	

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)	✔		
4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)			
4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)	✔		
4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)			✔
4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	✔		

หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

5.1.2 การควบคุมการเข้า-ออก (Physical entry controls)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบันมีการควบคุมการเข้า – ออกบริเวณห้องประมวลผล และที่เก็บข้อมูลสารสนเทศ โดยมีการใช้บัตรและรหัสผ่านเฉพาะสำหรับเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น และมีการกำหนดเวลาเข้าออกสำหรับผู้ที่ได้รับอนุญาตตามหน้าที่ที่รับผิดชอบ

5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารทรัพยากรบุคคล และฝ่ายบริหารงานทั่วไป

ข้อมูลที่ได้จากการสัมภาษณ์ : ก่อนทางเข้าสำนักงานในแต่ละชั้น พนักงานทุกท่านต้องทำการแปะบัตรผ่านก่อน เพื่อตรวจสอบสิทธิในการเข้าถึงในแต่ละพื้นที่ภายในองค์การฯ และนอกจากนี้ยังมี รปภ. เพื่อคอยตรวจสอบการนำของ เข้า-ออก และทำหน้าที่ประสานงานระหว่างผู้มาติดต่อจากภายนอกที่เข้ามาติดต่องานกับเจ้าหน้าที่ภายในองค์การฯ เพื่อป้องกันการเข้าพื้นที่โดยไม่รับอนุญาต

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารงานทั่วไป

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางตึกที่องค์การฯ ตั้งอยู่คือ อาคารชินวัตรทาวเวอร์ 3 ทางผู้ดูแลอาคารจะมีการซ้อมหนีไฟ ปีละ 2 ครั้ง โดยการประสานงานผ่านบริหารงานทั่วไปขององค์การฯ

5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายบริหารงานทั่วไป

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางอาคารชินวัตรทาวเวอร์ 3 จะมีการแลกบัตรสำหรับผู้มาติดต่อ โดยจะมีการแลกบัตร ตามบริษัทที่ต้องการมาติดต่อ ตั้งแต่ชั้น LOBBY และมีการรณรงค์ให้ท่านไหน ที่เป็นพนักงานของบริษัทต่างๆ ที่เช่าพื้นที่อาคารชินวัตร 3 ให้ติดบัตรพนักงานทุกครั้งที่มาทำงาน เพื่อง่ายต่อการตรวจสอบ โดยเจ้าหน้าที่ที่ทางอาคารได้จัดเตรียมไว้ และป้องกันบุคคลที่ไม่ประสงค์ดี ซึ่งอาจจะก่อให้เกิดความเสียหายได้

5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายคลัง และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการส่งส่งมอบสินค้า หรือระบบต่างๆ ทางองค์การฯ จะจัดพื้นที่ในการส่งมอบ พร้อมมีเจ้าหน้าที่ของทางหน่วยงานที่รับผิดชอบ หรือคณะกรรมการตรวจรับ คอยตรวจสอบอยู่อย่างใกล้ชิด

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการจัดการจัดวางอุปกรณ์ประมวลผลสารสนเทศ เช่น เครื่องคอมพิวเตอร์ เป็นต้น ทางเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ จะทำหน้าที่ในการติดตั้ง และให้คำแนะนำในการจัดวางสิ่งของ เพื่อป้องกันไม่ให้อุปกรณ์ประมวลผลสารสนเทศเกิดความเสียหาย

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในห้อง Server ซึ่งเป็นศูนย์รวมในการเก็บข้อมูล และเป็นห้องที่ติดตั้งเครื่องประมวลผลข้อมูลในระบบต่างๆ ซึ่งถือว่าเป็นห้องที่สำคัญมาก ทางฝ่ายเทคโนโลยีสารสนเทศ ได้มีการติดตั้งระบบกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศ และระบบควบคุมอุณหภูมิ เพื่อป้องกันความผิดพลาดที่จะเกิดขึ้น นอกจากนี้ยังมีการตรวจสอบความพร้อมใช้งานอยู่เสมอ

5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการเดินสายไฟฟ้า สายเคเบิ้ล รวมถึงสายที่ใช้ในระบบเครือข่ายภายในองค์การฯ ทั้งหมด จะถูกเดินสายและมีเครื่องป้องกันเพื่อไม่ให้เกิดอันตราย และไม่ให้เกิดอุปสรรคในการส่งผ่านสัญญาณ

5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในอุปกรณ์ทางด้านสารสนเทศทุกชนนิด จะมีการตรวจสอบสภาพการใช้งาน ให้พร้อมใช้งานอยู่อย่างสม่ำเสมอ โดยผู้เชี่ยวในแต่ละด้าน

5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการนำอุปกรณ์ทางด้านสารสนเทศไปใช้งานภายนอกสำนักงานแต่ละครั้ง จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศไปดำเนินการติดตั้ง และคอยแก้ไขปัญหาการให้ในการใช้งานแต่ละครั้งด้วย เพื่อป้องกันการใช้งานอย่างไม่ถูกต้อง และทำให้เกิดความเสียหายกับอุปกรณ์นั้นๆ

5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการกำจัดอุปกรณ์ หรือการหมุนเวียนนำอุปกรณ์สารสนเทศไปใช้ใหม่ เช่น มีการปรับเปลี่ยนผู้ใช้เครื่องคอมพิวเตอร์ เจ้าหน้าที่สารสนเทศต้องทำการล้างข้อมูลที่เป็นของผู้ใช้คนเดิมออกให้หมดก่อน

5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการนำอุปกรณ์ทางด้านสารสนเทศไปใช้งานนอกสำนักงาน ต้องได้รับการอนุมัติจากหัวหน้างานฝ่ายนั้นๆ อย่างเป็นลายลักษณ์ โดยใช้แบบฟอร์มที่ออกจากฝ่ายเทคโนโลยีสารสนเทศ และจะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศไปดำเนินการติดตั้ง และคอยแก้ไขปัญหาการให้ในการใช้งานแต่ละครั้ง และมีการกำหนดผู้รับผิดชอบอย่างชัดเจน และในการนำของออกนอกสำนักงานจะต้องผ่านการตรวจจากเจ้าหน้าที่รักษาความปลอดภัยของแต่ละชั้น อีกครั้ง เพื่อตรวจสอบว่าของที่นำออก ตรงกับเอกสารที่แจ้งไว้หรือไม่

ตารางที่ 4.12

ผลการสำรวจ

หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

(Physical and environmental security)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)			
5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)			✔
5.1.2 การควบคุมการเข้า-ออก (Physical entry controls)			✔
5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)			✔
5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)			✔
5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)			✔
5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)			✔
5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)			
5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)			✔
5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)			✔
5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)			✔

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)			✔
5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)			✔
5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)			✔
5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)			✔

หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communications and operations management)

6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ฝ่ายเทคโนโลยีสารสนเทศ ไม่มีการจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้องที่เป็นลายลักษณ์อักษร

6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ฝ่ายเทคโนโลยีสารสนเทศ ไม่มีการกำหนดการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือ แก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ มีการกำหนดหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต หรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน

6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการจัดทำข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ โดยจะระบุไว้ในสัญญาว่าจ้าง

6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการระบุเงื่อนไขในการให้บริการ ของหน่วยงานภายนอกไว้ในสัญญาว่าจ้าง และตรวจสอบผลการดำเนินงานตามสัญญา และในการแก้ไขแต่ละครั้งจะได้รับการบันทึก ตรวจสอบความถูกต้องของข้อมูล และแก้ไขจนกว่าระบบจะสามารถใช้งานได้ตามปกติ

6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : องค์การฯ มีมาตรการในการบริหารจัดการการเปลี่ยนแปลงจากหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)

6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศมีการสำรวจความต้องการเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตไว้ล่วงหน้า เพื่อกำหนดเป็นงบประมาณไว้ล่วงหน้าด้วย โดยการสำรวจจะแจ้งเป็นแบบฟอร์มไปยังแต่ละฝ่ายภายในองค์การฯ และให้ทางฝ่ายต่างๆ ระบุความต้องการและต้องได้รับการอนุมัติจากผู้มีอำนาจด้วย

6.3.2 การตรวจรับระบบ (System acceptance)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการตรวจรับระบบงานต่างๆ จะการตั้งคณะกรรมการเพื่อทำการตรวจรับ ตามขั้นตอน เพื่อให้ตรงตามคุณลักษณะที่กำหนดอย่างละเอียด และต้องทดสอบการใช้งานว่าสามารถใช้งานได้สมบูรณ์ และเอกสารจะต้องได้รับการอนุมัติจากผู้อำนวยการองค์การฯ ด้วย

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)

6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ได้จัดทำระบบป้องกัน ตรวจจับโปรแกรมที่ไม่ประสงค์ดี และมีการจัดทำรายงานผลทุกสัปดาห์ และมีการอบรมให้ความรู้แก่พนักงานภายในเพื่อให้ตระหนัก และให้พนักงานรู้จักป้องกันตัวเองจากภัยคุกคามในด้านต่างๆ ด้วย

6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้ โดยมีการติดตั้งโปรแกรมป้องกันไว้ยังเครื่องคอมพิวเตอร์ทุกเครื่อง

6.5 การสำรองข้อมูล (Back-up)

6.5.1 การสำรองข้อมูล (Information back-up)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน ทางองค์การฯ ยังไม่มีการตารางสำหรับบันทึกการสำรอง ว่ามีความครบถ้วน สมบูรณ์ สม่ำเสมอหรือไม่ และไม่มีการทดสอบความพร้อมใช้งานของข้อมูลที่ทำการสำรองไว้

6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

6.6.1 มาตรการทางเครือข่าย (Network controls)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ไม่มีกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์การฯ ใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์การฯ เองหรือบริการที่ได้รับจากหน่วยงานภายนอก

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)

6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : กำลังมีการจัดทำมาตรการ หรือขั้นตอนเพื่อนำไปปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เช่น การออกนโยบาย และประชาสัมพันธ์ให้ความรู้ ในกรณีที่ต้องการนำสื่อบันทึกข้อมูลเคลื่อนที่ได้มาใช้ภายในองค์การฯ ควรมีการสแกนไวรัส ก่อนนำมาใช้เชื่อมต่อกับเครื่องคอมพิวเตอร์ภายในองค์การฯ

6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ไม่มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ กำลังดำเนินการกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต อย่างเป็นลายลักษณ์อักษร

6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)

6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

ผู้ให้สัมภาษณ์ : กลุ่มผู้บริหารองค์การฯ และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน องค์การฯ ยังไม่มีการกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร

6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน องค์การฯ ยังไม่มีการจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กร อย่างเป็นลายลักษณ์อักษร

6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางองค์การฯ ยังไม่มีออกกฎระเบียบ หรือบทลงโทษ หรือวางมาตราป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์การฯ

6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ กำลังจัดทำมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ยังไม่มีการกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ไม่มีการจัดทำมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่าน

ทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ไม่มีการกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ไม่มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศ ไม่มีการกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย อย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ไม่มีการกำหนดขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ไม่มีการกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การ ฯ ไม่มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศขององค์การ ฯ ไม่มีการกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบันทางฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ได้มีการจัดทำระบบในการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

ตารางที่ 4.13

ผลการสำรวจ

หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ

(Communications and operations management)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)			
6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	✔		
6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ ประมวลผลสารสนเทศ (Change management)	✔		
6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)			✔
6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)			✔
6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)			
6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)			✔
6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)			✔
6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)			✔
6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)			
6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)			✔
6.3.2 การตรวจรับระบบ (System acceptance)			✔

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)			
6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)			✔
6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)			✔
6.5 การสำรองข้อมูล (Back-up/Housekeeping)			
6.5.1 การสำรองข้อมูล (Information back-up)	✔		
6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)			
6.6.1 มาตรการทางเครือข่าย (Network controls)	✔		
6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)	✔		
6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling and security)			
6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)		✔	
6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	✔		
6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)		✔	
6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)	✔		
6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)			
6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)	✔		
6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)	✔		
6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)	✔		

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)		✔	
6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)	✔		
6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)			
6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)	✔		
6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)	✔		
6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)	✔		
6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)			
6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)	✔		
6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)	✔		
6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)	✔		
6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)	✔		
6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)	✔		
6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)			✔

หมวดที่ 7 การควบคุมการเข้าถึง (Access control)

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ขององค์การฯ ยังไม่มีการจัดทำนโยบายควบคุมการเข้าถึงระบบ หรือข้อมูลสารสนเทศอย่างเป็นลายลักษณ์อักษร

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

7.2.1 การลงทะเบียนพนักงาน (User registration)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการลงทะเบียนพนักงานจะรวมถึงการเข้าใช้ระบบ และการถอดสิทธิการใช้งานด้วย แต่ ณ ปัจจุบัน จะมีแต่การกรอกแบบฟอร์มขอเข้าใช้ระบบงาน และระบุสิทธิที่ต้องการเข้าใช้งาน แต่ยังถึงว่าการปฏิบัติตาม ISO27001 ในข้อนี้ยังไม่สมบูรณ์ เนื่องจากเวลาถอดสิทธิการใช้งานไม่การยื่นแบบฟอร์ม และแจ้งมาเป็นลักษณ์อักษร

7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ถึงแม้องค์การฯ จะมีการกำหนดสิทธิในการเข้าใช้งานระบบสารสนเทศภายในองค์การฯ แต่เนื่องจากยังไม่มีกระบวนการถอดสิทธิผู้ที่ไม่สิทธิเข้าใช้งาน เช่น ลาออก เป็นต้น ดังนั้นใน ISO27001 ยังไม่สมบูรณ์

7.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ขององค์การฯ ยังไม่มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ขององค์การฯ ยังไม่มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

7.3.1 การใช้งานรหัสผ่าน (Password use)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ขององค์การฯ ยังไม่มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน และไม่มีการอบรมให้ความรู้เกี่ยวกับการรักษาความลับของรหัสผ่านของแต่ละบุคคล

7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ขององค์การยังไม่มีการจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ไม่มีการจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้

7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการเข้าใช้เครือข่ายที่มาจากภายนอกจะมีการพิสูจน์ตัวตนโดยการกำหนดรหัสผ่าน และกำหนดสิทธิในการเข้าใช้งานให้เป็นรายบุคคล โดยจะต้องได้รับอนุญาตจากผู้มีอำนาจเท่านั้น

7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการเชื่อมต่อเพื่อใช้ข้อมูลบนเครือข่ายภายในองค์การฯ จะต้องมีการพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : องค์การฯ มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการได้ครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย โดยจะทำการเปิดให้เข้าถึงพอร์ตเฉพาะที่ใช้งานจริงเท่านั้น และกำหนดสิทธิของผู้เข้าใช้งานพอร์ตนั้นเป็นรายบุคคล

7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศมีการแบ่งแยกเครือข่ายตามกลุ่มตามผู้ใช้งาน

7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : มีการจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย โดยจะอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากองค์การฯ ยังไม่มีนโยบายควบคุมการเข้าถึง จึงยังไม่การกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่าย และการไหลเวียนของสารสนเทศบนเครือข่าย

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ยังไม่มีการกำหนดขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ จัดให้ผู้ต้องการใช้งานระบบสารสนเทศต่างๆ ต้องผ่านกระบวนการในการพิสูจน์ตัวตนก่อนการเข้าใช้งานทุกครั้ง

7.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ยังไม่มีการจัดทำระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน องค์การกำลังมีการจัดทำวิธีการในการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ขององค์การฯ ยังไม่มีการกำหนดให้มีระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ ขององค์การ ฯ ยังไม่มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)

7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ผู้ที่ต้องการเข้าถึงสารสนเทศข้อมูล หรือแอพพลิเคชั่นภายในองค์การฯ จะต้องกรอกแบบฟอร์มในการขอเข้าใช้ ส่งมายังฝ่ายเทคโนโลยีสารสนเทศ จากนั้นจะทำการเปิดให้ใช้งานตามความจำเป็น และต้องเป็นผู้ที่ได้รับการอนุมัติจากผู้มีอำนาจเท่านั้น

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบันยังไม่มีการแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ อยู่ระหว่างการกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น)

7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ตารางที่ 4.14
ผลการสำรวจ
หมวดที่ 7 การควบคุมการเข้าถึง
(Access control)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)			
7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	✔		
7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
7.2.1 การลงทะเบียนพนักงาน (User registration)		✔	

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)		✔	
7.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	✔		
7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	✔		
7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			
7.3.1 การใช้งานรหัสผ่าน (Password use)	✔		
7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)	✔		
7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)	✔		
7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)			
7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	✔		
7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)			✔
7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)			✔
7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)			✔
7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)			✔
7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)			✔
7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)	✔		

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)		✔	
7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)			✔
7.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)	✔		
7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)		✔	
7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	✔		
7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)	✔		
7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)			
7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)			✔
7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	✔		
7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)		✔	
7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน *(Teleworking)*	✔		

หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)

8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน ฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ยังไม่มีการวิเคราะห์ และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ๆ หรือการปรับปรุงจากระบบที่มีอยู่แล้ว

8.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)

8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน องค์การฯ ไม่มีมาตรการสำหรับการตรวจสอบข้อมูลนำเข้าของแอพพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลหรือไม่

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบัน องค์การฯ ไม่มีมาตรการสำหรับการตรวจสอบความผิดพลาดของข้อมูลที่อยู่ในระหว่างการประมวลผลแอพพลิเคชั่นต่างๆ

8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน องค์การฯ ยังไม่มีมาตรการในการตรวจสอบความถูกต้องของข้อมูล รวมถึงมาตรการป้องกันการเปลี่ยนแปลงหรือการเข้าไปแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการนำข้อมูลออกจากแอพพลิเคชั่น ในแต่ละครั้ง องค์การฯ ยังไม่มีมาตรการการตรวจสอบความถูกต้องของข้อมูล

8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ทางฝ่ายเทคโนโลยีสารสนเทศ ยังไม่มีการจัดทำนโยบายในการเข้ารหัสข้อมูล

8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน องค์การฯ ไม่มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เมื่อทางผู้พัฒนาระบบ ดำเนินการพัฒนาระบบเสร็จเรียบร้อยแล้ว จนถึงขั้นตอนในการทดสอบระบบก่อนการใช้งานจริง ซึ่งทางฝ่ายเทคโนโลยี

สารสนเทศ ได้จัดให้มีเครื่องมือ หรืออุปกรณ์ที่ใช้ในการทดสอบแยกออกจากระบบจริง และข้อมูลก็จะเป็นข้อมูลที่ใช้ในการทดสอบ เมื่อทดสอบจนครบถ้วนสมบูรณ์แล้วจึงนำไปใช้กลับระบบจริง

8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศ มีมาตรการในการป้องกันซอร์สโค้ดของระบบ โดยการกำหนดรหัสผ่าน และให้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้นในการเข้าถึง

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)

8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ปัจจุบันยังไม่มีการกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ

8.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบัน องค์การฯ มีการตรวจสอบทางเทคนิคในการใช้งานแอพพลิเคชั่นก่อน สำหรับเครื่องที่มีการปรับเปลี่ยนระบบปฏิบัติการ

8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ก่อนการแก้ไข หรือเปลี่ยนแปลงซอฟต์แวร์ที่มาจากภายนอก จะถูกควบคุมโดยสัญญาการว่าจ้าง และก่อนการแก้ไขทุกครั้งทางเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ จะทำการสำรองข้อมูลไว้ก่อนทุกครั้งที่จะมีการเปลี่ยนแปลง

8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบันองค์การฯ ไม่มีการกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป

8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก ทางองค์การฯ ได้มีการจัดตั้งคณะกรรมการขึ้นตามความชำนาญของแต่ละระบบ เพื่อทำการคัดสรรและตรวจสอบ การพัฒนาซอฟต์แวร์ที่มาจากหน่วยงานภายนอก

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในปัจจุบันองค์การฯ ยังไม่มีการประเมินความเสี่ยงที่เกิดจะเกิดช่องโหว่ และไม่มีการกำหนดมาตรการรองรับเพื่อลดความเสี่ยง

ตารางที่ 4.15

ผลการสำรวจ

หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(Information systems acquisition, development and maintenance)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)			
8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)	✔		

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
8.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)			
8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)	✔		
8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)	✔		
8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)	✔		
8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)	✔		
8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)			
8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)	✔		
8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)	✔		
8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)			
8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)	✔		
8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)			✔
8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)			✔
8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)			
8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)	✔		
8.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)			✔

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)			✔
8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)	✔		
8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)			✔
8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)			
8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)	✔		

หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน ทางฝ่ายเทคโนโลยีสารสนเทศ ยังไม่มีการกำหนดช่องทางในการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่หลากหลาย และเป็นทางการ โดยส่วนใหญ่จะใช้เป็นการ ติดต่อผ่านทางเบอร์โทรภายใน แจ้งมายังฝ่ายเทคโนโลยีสารสนเทศ เมื่อเกิดปัญหาขึ้นเท่านั้น ซึ่งบางครั้งเจ้าหน้าที่อาจไม่อยู่ทำให้ไม่ได้รับการแจ้งปัญหาอย่างทันถ่วงที

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน ทางผู้ใช้งาน ไม่มีการ รายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การฯ เมื่อสังเกตพบ หรือเกิดความสงสัยในการใช้งานระบบ ส่วนใหญ่มักจะรอให้เกิดปัญหาขึ้นก่อน แล้วจึงแจ้งมายังเจ้าหน้าที่เพื่อให้ดำเนินการแก้ไข และเมื่อแก้ไขแล้ว และทางเจ้าหน้าที่ฝ่ายสารสนเทศเอง หลังจากที่ทำการแก้ไขแล้ว ไม่มีการบันทึกถึงปัญหาที่เกิดขึ้น ทำให้ไม่มีรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การฯ ที่เป็นลายลักษณ์อักษร

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากไม่มีการเก็บรวบรวมข้อมูลถึงปัญหาที่เกิดขึ้นเกี่ยวกับความมั่นคงปลอดภัย จึงยังไม่มีการกำหนดหน้าที่ ความรับผิดชอบ หรือระเบียบขั้นตอนปฏิบัติงานที่ชัดเจน และเป็นลายลักษณ์อักษร

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน ฝ่ายเทคโนโลยีสารสนเทศขององค์การฯ ไม่มีการบันทึกเหตุการณ์ที่เป็นละเมิดความมั่นคงปลอดภัย รวมถึงยังไม่มีการแยกประเภทของเหตุการณ์ ปริมาณที่เกิด ค่าใช้จ่ายที่เกิดขึ้น

9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจาก ในการแก้ไขปัญหาในแต่ละครั้งไม่มีการบันทึกข้อมูลไว้ จึงทำให้หลักฐานอ้างอิงต่างๆ ยังไม่สมบูรณ์

ตารางที่ 4.16

ผลการสำรวจ

หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)			
9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)	✔		
9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	✔		
9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)			
9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)	✔		
9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)	✔		
9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)	✔		

หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)

10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : องค์การฯ ยังไม่มีกระบวนในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการ

10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : องค์การฯ ยังไม่มีการประเมินความเสี่ยงที่อาจเกิดขึ้น ที่จะส่งผลต่อความมั่นคงปลอดภัยสำหรับสารสนเทศภายในองค์การ

10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ

10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากยังไม่มีการกำหนดแผนงานในการสร้างความต่อเนื่องให้กับธุรกิจ จึงยังไม่การทดสอบและทบทวนแผนดังกล่าว

ตารางที่ 4.17

ผลการสำรวจ

หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

(Business continuity management)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)			
10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)	✔		
10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	✔		
10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)	✔		
10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)	✔		
10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)	✔		

หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากมีการประกาศใช้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และทางองค์การฯ เองเข้าข่ายผู้ที่ต้องปฏิบัติตามกฎหมาย ที่ผ่านมา ฝ่ายเทคโนโลยีสารสนเทศ ได้มีการจัดอบรมให้ความรู้แก่พนักงานเกี่ยวกับ พรบ. ดังกล่าว และขณะนี้ กำลังอยู่ในระหว่างกำหนดข้อปฏิบัติที่พนักงานจะต้องปฏิบัติตามที่เป็นลายลักษณ์อักษร และจะนำออกประกาศใช้ และมีพนักงานลงนามทราบ

11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP))

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการในการจัดหาซอฟต์แวร์ ที่ใช้งานภายในองค์การฯ อย่างถูกต้องตามกฎหมาย และจะเป็นผู้ดำเนินการติดตั้งให้กับผู้ใช้งาน และกำหนดสิทธิไม่ให้ผู้ใช้งานทั่วไป มีสิทธิในการลงโปรแกรมเอง เป็นการป้องกันการลงโปรแกรมที่ไม่ถูกต้อง หรือผิดกฎหมาย

11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ยังไม่มีการกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนด

11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากระเบียบปฏิบัติ และข้อกำหนดอยู่ระหว่างการจัดทำ รวมถึงยังไม่มีการแบ่งประเภทของข้อมูล จึงยังไม่ข้อกำหนดเพื่อป้องกันข้อมูลส่วนตัว

11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ในการขอใช้งานอุปกรณ์ประมวลสารสนเทศภายในองค์การฯ จะต้องกรอกแบบฟอร์มขอใช้ พร้อมระบุเหตุผล การใช้งานของอุปกรณ์อย่างละเอียดตามที่แบบฟอร์มกำหนด ซึ่งแบบฟอร์มคำขอใช้ จะถูกพิจารณาจากหัวหน้างานของฝ่ายผู้ขอ

จากนั้นจะถูกพิจารณาจาหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ อีกครั้ง ก่อนที่จะอนุญาตให้นำอุปกรณ์ไปใช้งาน เพื่อป้องกันการใช้อุปกรณ์ผิดวัตถุประสงค์

11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากองค์การฯ ยังไม่มีการระบุข้อกำหนดทางกฎหมายที่ชัดเจน จึงทำให้บางระบบงานยังไม่มีการเข้ารหัสข้อมูล ก่อนการนำไปใช้งาน

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)

11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : เนื่องจากนโยบายทางด้านมาตรฐานความมั่นคงปลอดภัยขององค์การฯ ยังไม่มีการจัดทำอย่างเป็นลายลักษณ์อักษร และไม่มีการประกาศใช้อย่างเป็นทางการ จึงยังไม่มีข้อกำหนดให้ผู้บังคับบัญชาใช้บังคับกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน

11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ที่ผ่าน ทางองค์การฯ ยังไม่มีการนำมาตรฐานมาใช้ในการตรวจสอบระบบสารสนเทศขององค์การฯ

11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)

11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : ณ ปัจจุบัน องค์การฯ อยู่ระหว่างการถูกตรวจประเมินจากผู้ตรวจสอบภายใน ซึ่งอยู่ระหว่างขั้นตอนการศึกษา รวมรวบข้อมูล เพื่อนำไประบุเป็นข้อกำหนดกิจกรรมที่เกี่ยวข้องกับการตรวจประเมิน และกำหนดช่วงเวลาในการตรวจที่เหมาะสมเพื่อให้เกิดผลกระทบกับกระบวนในการทำงานน้อยที่สุด

11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)

ผู้ให้สัมภาษณ์ : หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ข้อมูลที่ได้จากการสัมภาษณ์ : อยู่ระหว่างการจัดหา เครื่องมือที่ใช้ในการตรวจประเมินเพื่อให้เหมาะสม กับระบบ ซึ่งจะทำให้การข้อมูลที่ได้จากเครื่องมือดังกล่าวถูกต้องตามวัตถุประสงค์ และน่าเชื่อถือมากที่สุด

ตารางที่ 4.18 ผลการสำรวจ

หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)			
11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)		✔	
11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP))			✔
11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)	✔		
11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)	✔		
11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)	✔		

ผลการสำรวจการดำเนินการ	ยังไม่เริ่ม	กำลัง	แล้วเสร็จ
11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)	✔		
11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)			
11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)	✔		
11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)	✔		
11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)			
11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)		✔	
11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)		✔	

3. ผลการสำรวจความคิดเห็น ด้านการรักษาความปลอดภัยระบบสารสนเทศในองค์การตามมาตรฐาน ISO/IEC27001

เป็นการสำรวจข้อมูลโดยใช้แบบสอบถาม เพื่อสำรวจความคิดเห็นของกลุ่มตัวอย่าง จำนวนทั้งสิ้น 285 คน ที่มีต่อการดำเนินงานทางด้านเทคโนโลยีสารสนเทศในปัจจุบัน ตามกรอบมาตรฐาน ISO/IEC27001

ตารางที่ 4.19

ผลการสำรวจความคิดเห็นของพนักงาน

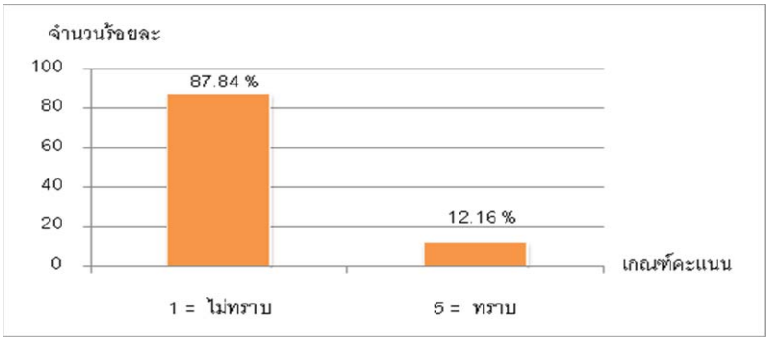
หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ

ผลการสำรวจความคิดเห็นหมวดที่ 1	1 ไม่ทราบ	5 ทราบ
ท่านทราบหรือไม่ว่าปัจจุบันองค์การมีการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร (กรณีที่ไม่ทราบ ข้ามไปทำหมวดต่อไป) (1 = ไม่ทราบ , 5 = ทราบ)	241	44
ท่านทราบรายละเอียดของนโยบายดังกล่าวหรือไม่ (1 = ไม่ทราบ , 5 = ทราบ)	255	30
ท่านทราบแหล่งที่สามารถเข้าไปอ่านนโยบายดังกล่าวหรือไม่ (1 = ไม่ทราบ , 5 = ทราบ)	255	30
รวม	751	104
% เฉลี่ยรวม	87.84	12.16

ภาพที่ 4.8

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ



ตารางที่ 4.20

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

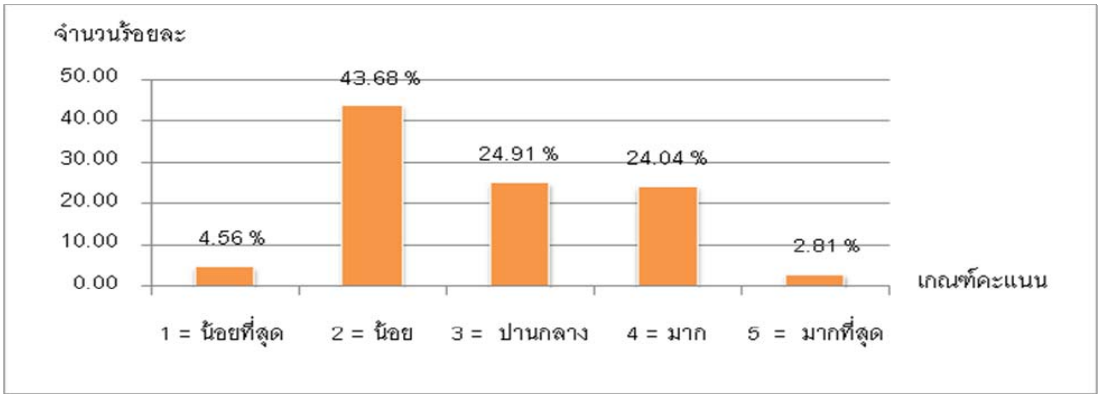
หมวดที่ 2 ด้านโครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์การ (Internal Organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

ผลการสำรวจความคิดเห็นหมวดที่ 2	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านทราบหน้าที่ความรับผิดชอบของท่านในการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยเพียงใด	14	195	53	19	4
ท่านคิดว่ากระบวนการขอใช้อุปกรณ์ประมวลผลสารสนเทศ มีขั้นตอนที่เหมาะสมหรือไม่	12	30	81	160	2
ท่านทราบเรื่องการรักษาและไม่เปิดเผยความลับขององค์การมากน้อยเพียงใด	18	150	64	38	15
ท่านคิดว่าผู้บริหารองค์การ ให้ความสำคัญกับการบริหารจัดการด้านความมั่นคงปลอดภัยทางด้านระบบสารสนเทศภายในองค์การมากน้อยเพียงใด	8	123	86	57	11
รวม	52	498	284	274	32
% เฉลี่ยรวม	4.56	43.68	24.91	24.04	2.81

ภาพที่ 4.9

กราฟร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 2 ด้านโครงสร้างทางด้านความมั่งคงปลอดภัยภายในองค์การ (Internal Organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)



ตารางที่ 4.21

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

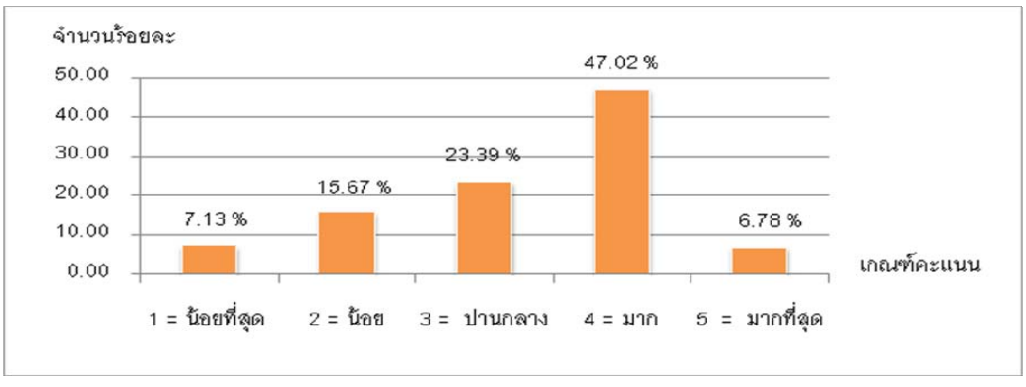
หมวดที่ 3 ด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์การ (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)

ผลการสำรวจความคิดเห็นหมวดที่ 3	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าองค์การมีการระบุความเป็นเจ้าของในอุปกรณ์สารสนเทศ อย่างชัดเจน	6	26	51	195	7
ท่านทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์การ สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศมากน้อยแค่ไหน	10	42	56	132	45
ท่านสามารถแบ่งประเภทของข้อมูลได้มากน้อยแค่ไหน เช่น ข้อมูลลับ(Secret Information),ข้อมูลลับเฉพาะ (Confidential Information),ข้อมูลที่จำเป็นมาก(Critical Information),ข้อมูลสาธารณะหรือข้อมูลทั่วไป	45	66	93	75	6
รวม	61	134	200	402	58
% เฉลี่ยรวม	7.13	15.67	23.39	**47.02**	6.78

ภาพที่ 4.10

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 3 ด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์การ (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)



ตารางที่ 4.22

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

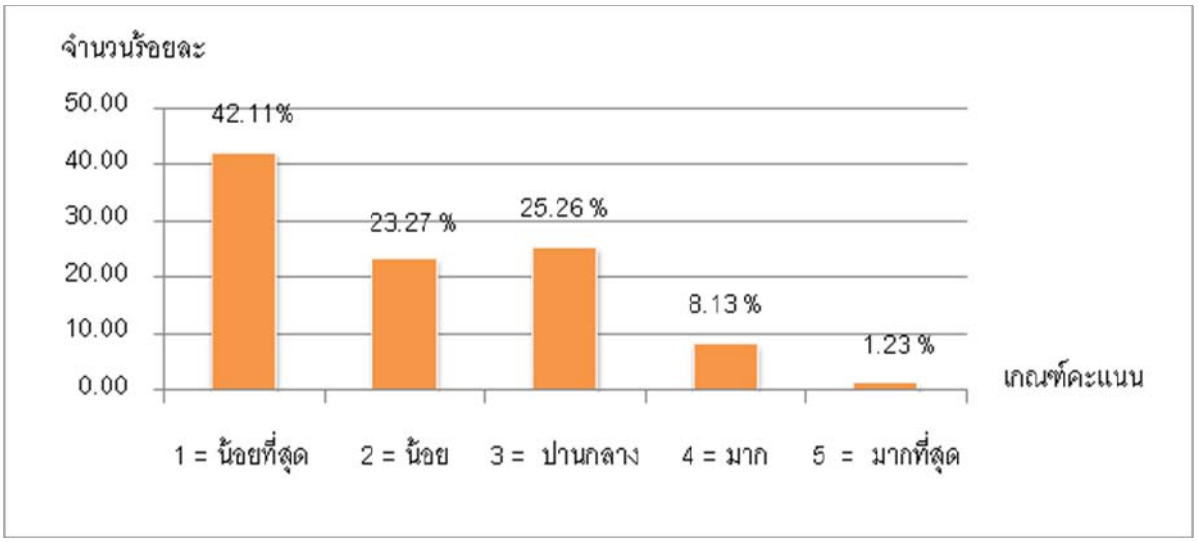
หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการ จ้างงาน (During employment)

ผลการสำรวจความคิดเห็นหมวดที่ 4	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ต่างๆ ภายในองค์การมีความเหมาะสมเพียงใด	56	52	156	19	2
ท่านเคยได้รับการฝึกอบรมหรือรับความรู้ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยแค่ไหน	156	89	25	15	0
ท่านคิดว่าคุณสมบัติของผู้ให้บริการทางด้านสารสนเทศมีความรู้ความสามารถเหมาะสมกับงานมากน้อยแค่ไหน	72	61	89	58	5
ท่านทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายระเบียบปฏิบัติทางด้านความปลอดภัยขององค์การมากน้อยแค่ไหน	185	18	65	12	5
ท่านคิดว่ากระบวนการคืนทรัพย์สินขององค์การ มีความเหมาะสมและครบถ้วนมากน้อยเพียงใด	95	103	56	27	4
ท่านคิดว่ามาตรการในการถอดสิทธิ์การเข้าใช้งาน ระบบและโปรแกรมประยุกต์ (Application)ต่างๆ สำหรับพนักงานลาออกไปแล้ว อยู่ในระดับที่เหมาะสมเพียงใด	156	75	41	8	5
รวม	720	398	432	139	21
% เฉลี่ยรวม	42.11	23.27	25.26	8.13	1.23

ภาพที่ 4.11

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการ จ้างงาน (During employment)



ตารางที่ 4.23

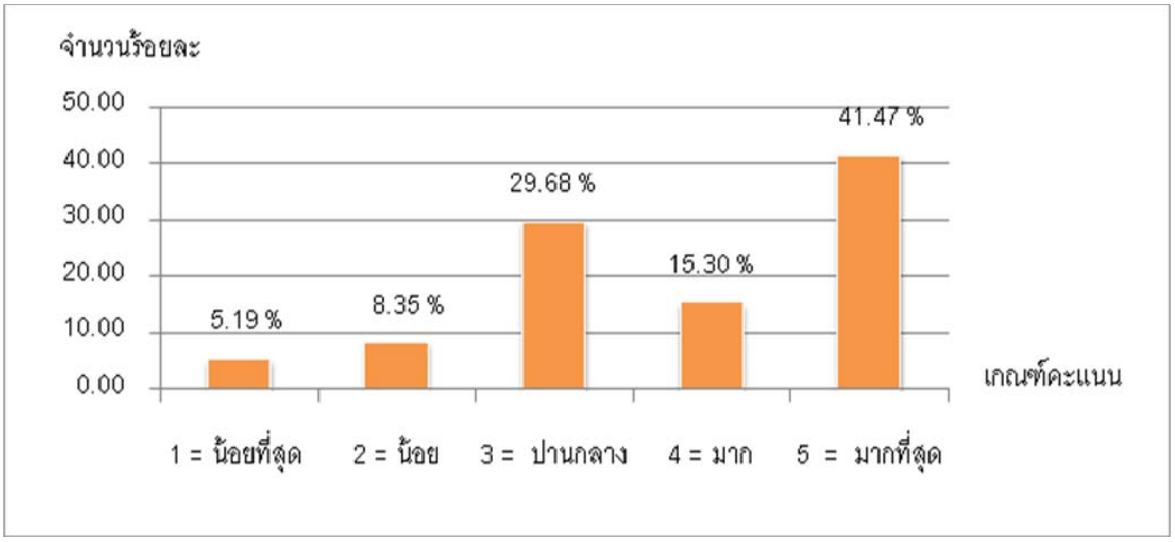
ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 5 ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

ผลการสำรวจความคิดเห็นหมวดที่ 5	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าปัจจุบันบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศขององค์การที่สำคัญ มีความเหมาะสมหรือความปลอดภัยมากน้อยเพียงใด	0	0	56	42	187
ท่านคิดว่าการจัดทำบริเวณ ล้อมรอบ การเข้าถึงอุปกรณ์สารสารเทศ ภายในองค์การมีความเหมาะสมเพียงใด	2	5	65	66	147
ท่านคิดว่าการควบคุมการเข้า - ออกบริเวณพื้นที่สำคัญหรือที่ต้องการรักษาควบปลอดภัยมีความเหมาะสมหรือปลอดภัยมากน้อยเพียงใด	42	20	39	12	172
ท่านมีการระวังและป้องกันอุบัติเหตุต่างๆ มากน้อยเพียงใด เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชน หรือ เสี่ยงต่อการเกิดเข้าใช้งานจากผู้ไม่มีสิทธิเป็นต้น	20	42	121	62	40
ท่าคิดว่าองค์กรมีการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานมากน้อยเพียงใด	10	52	142	36	45
รวม	74	119	423	218	591
% เฉลี่ยรวม	5.19	8.35	29.68	15.30	**41.47**

ภาพที่ 4.12

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 5 ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)



ตารางที่ 4.24

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 6 ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and Operations Management)

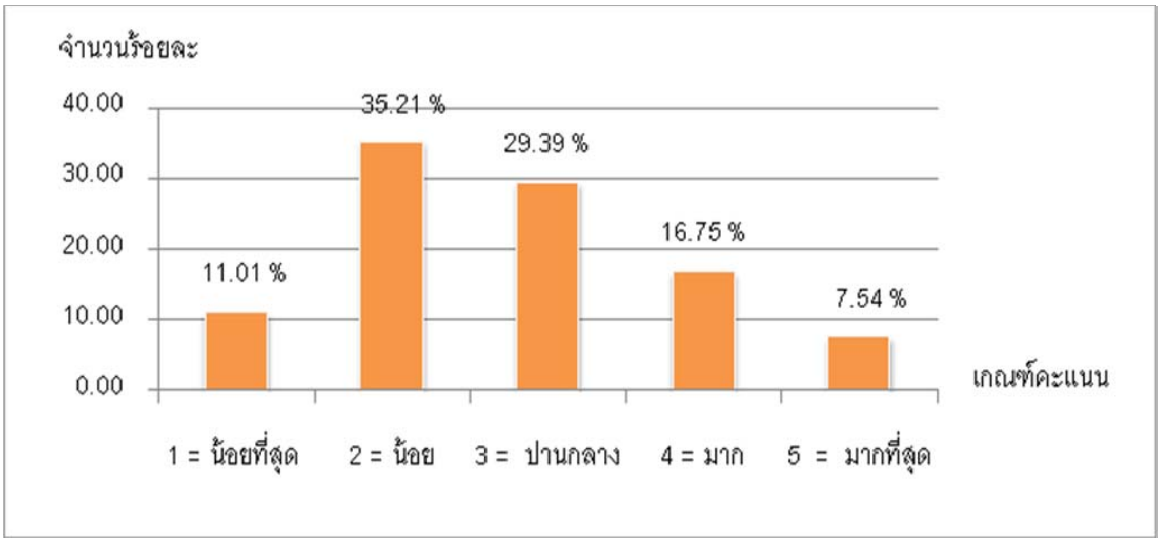
ผลการสำรวจความคิดเห็นหมวดที่ 6	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
หน่วยงานของท่านมีการปรับปรุงคู่มือขั้นตอนการปฏิบัติงาน (Documented Operating Procedures)ตามระยะเวลาอันสมควรสม่ำเสมอมากน้อยเพียงใด	23	134	66	42	20
ท่านเห็นว่าองค์กรมีการบริหารจัดการเครือข่าย (Network Control) และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application)	56	174	25	30	0

ผลการสำรวจความคิดเห็นหมวดที่ 6	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านให้ความสำคัญในการจัดเก็บเอกสารหรือข้อมูลต่างๆ ในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องมากน้อยเพียงใด	15	24	125	85	36
ท่านทราบกฎระเบียบ ข้อบังคับสิทธิของการส่งข้อมูลต่างๆ ออกไปนอกองค์กรมากน้อยเพียงใด	45	159	58	23	0
ท่านทราบกฎระเบียบ ข้อบังคับสิทธิของการใช้อินเตอร์เน็ตขององค์กรมากน้อยเพียงใด	56	56	142	25	6
ท่านทราบกฎระเบียบ ข้อบังคับ สิทธิของการใช้อีเมล์ขององค์กรมากน้อยเพียงใด	21	87	74	55	48
ท่านเห็นว่าองค์กรมีการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT สม่ำเสมอมากน้อยเพียงใด	15	96	90	67	17
ท่านคิดว่าเครื่องคอมพิวเตอร์ภายในองค์การ มีการตั้งเวลาได้ถูกต้อง แม่นยำมากน้อยแค่ไหน	20	75	90	55	45
รวม	251	805	670	382	172
% เฉลี่ยรวม	11.01	**35.31**	29.39	16.75	7.54

ภาพที่ 4.13

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 6 ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and Operations Management)



ตารางที่ 4.25

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 7 ด้าน การควบคุมการเข้าถึง (Access Control)

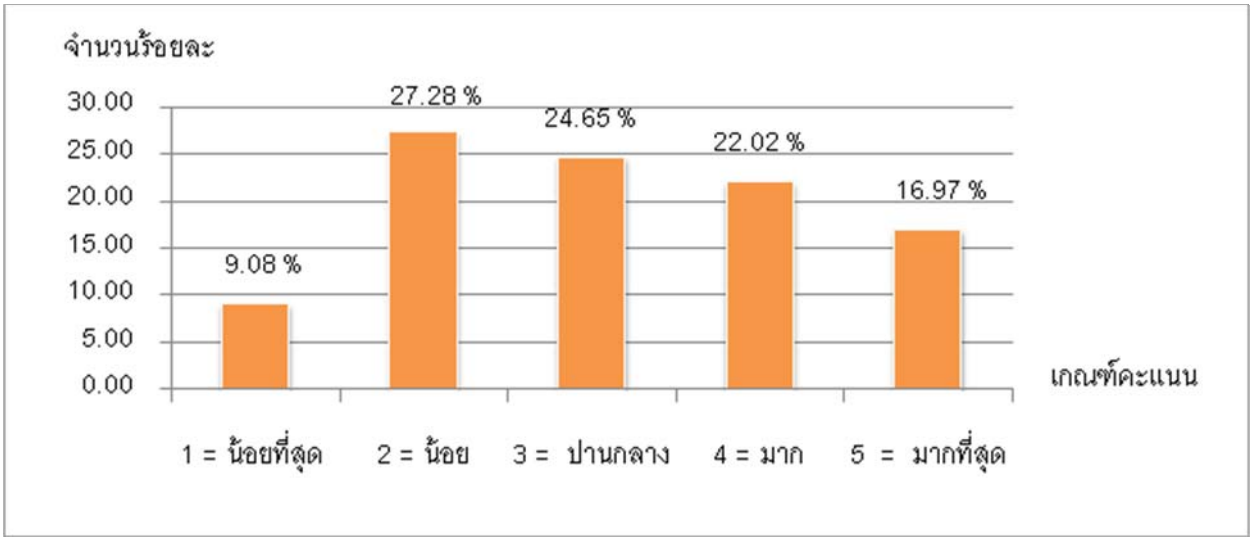
ผลการสำรวจความคิดเห็นหมวดที่ 7	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์กรมากน้อยเพียงใด	56	123	27	59	20
ถ้าองค์กรมีการแจ้ง หรือสรุป สิทธิการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์กร ให้ท่านทราบตามระยะที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) ท่านเห็นด้วยมากน้อยเพียงใด	0	5	85	58	137

ผลการสำรวจความคิดเห็นหมวดที่ 7	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านให้ความสำคัญกับการ Log Off เครื่อง หรือปิดเครื่อง เมื่อท่านไม่อยู่เป็นเวลานาน เช่น ประชุม , ทานอาหารกลางวัน มากน้อยเพียงใด	10	85	78	65	47
ท่านให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ท่านใช้งานมากน้อยเพียงใด	0	4	99	58	124
ท่านให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆ ขององค์กรมากน้อยเพียงใด	25	97	54	85	24
ท่านเห็นว่ามาตรฐานการใส่ User ID & Password ก่อนเข้าใช้งานระบบต่างๆ ภายในองค์กร (ระบบบริหารจัดการรหัสผ่าน - Password Management System) มีความเหมาะสมและปลอดภัยมากน้อยเพียงใด	68	167	25	25	0
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆ ขององค์การมากน้อยเพียงใด	36	37	111	78	23
ท่านมีการตรวจสอบอุปกรณ์ต่อพ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์การมากน้อยเพียงใด ตัวอย่าง การ Scan ไวรัสใน HandDrive ก่อนใช้งาน ฯลฯ	12	104	83	74	12
รวม	207	622	562	502	387
% เฉลี่ยรวม	9.08	**27.28**	24.65	22.02	16.97

ภาพที่ 4.14

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 7 ด้าน การควบคุมการเข้าถึง (Access Control)



ตารางที่ 4.26

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance)

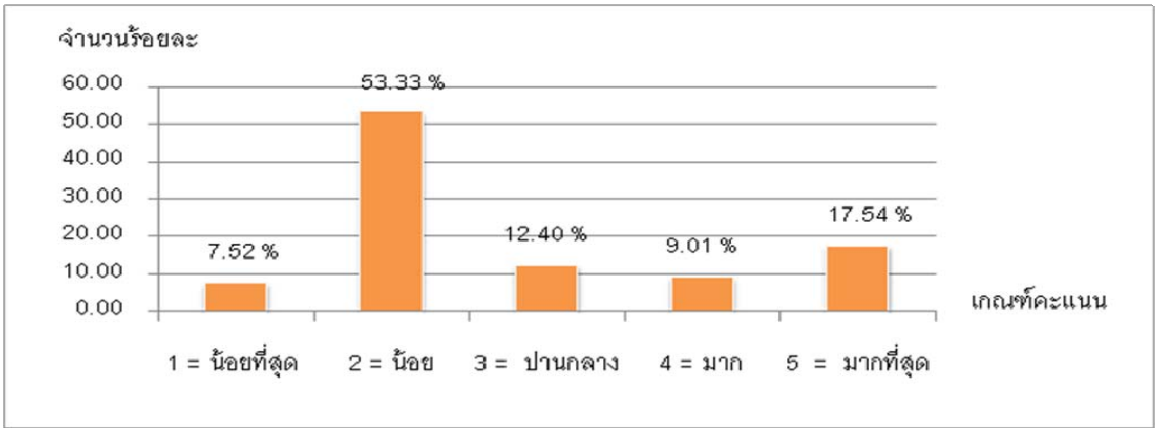
ผลการสำรวจความคิดเห็นหมวดที่ 8	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเคยประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลบ้างหรือไม่และมากน้อยเพียงใด (1 =ไม่เคย 0% , 2 = พบประมาณ 1 - 25 % , 3 = พบประมาณ 26 - 50 % , 4 = พบประมาณ 51 - 75 % , 5 = พบประมาณ 76 - 100 %)	21	144	58	21	41

ผลการสำรวจความคิดเห็นหมวดที่ 8	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเคยประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนบ้างหรือไม่และมากน้อยเพียงใด(1 =ไม่เคย 0% , 2 = พบประมาณ 1 - 25 % , 3 = พบประมาณ 26 - 50 % , 4 = พบประมาณ 51 - 75 % , 5 = พบประมาณ 76 - 100 %)	45	162	48	20	10
ท่านเคยประสบปัญหาต่างๆ ดังกล่าว ท่านได้ทำการแจ้งทีมงานผู้ดูแลผ่านช่องทางที่กำหนดหรือไม่ (1 =ไม่เคย 0% , 2 = แจ้งประมาณ 1 - 25 % , 3 = แจ้งประมาณ 26 - 50 % , 4 = แจ้งประมาณ 51 - 75 % , 5 = แจ้งประมาณ 76 - 100 %)	0	150	0	36	99
รวม	66	456	106	77	150
% เฉลี่ยรวม	7.72	53.33	12.40	9.01	17.54

ภาพที่ 4.15

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance)



ตารางที่ 4.27

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 9 ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การ (Information Security Incident Management)

ผลการสำรวจความคิดเห็นหมวดที่ 9	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าซอฟต์แวร์ป้องกันไวรัสและมาตรการต่างๆ ในการป้องกันไวรัสขององค์การมีความเหมาะสมมากน้อยเพียงใด	199	66	20	0	0
ท่านเคยรายงานเหตุการณ์หรือรายงานจุดอ่อน จุดบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่มากน้อยเพียงใด	0	42	145	86	12

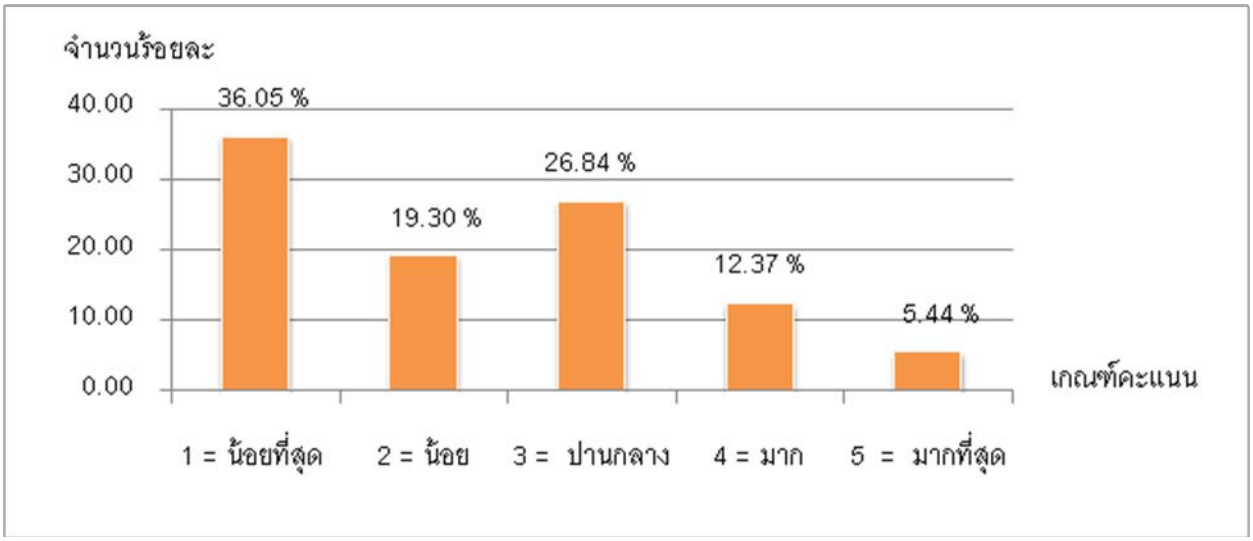
ผลการสำรวจความคิดเห็นหมวดที่ 9	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่า ทางส่วนงานเทคโนโลยีสารสนเทศ การรายงานถึงข้อผิดพลาดและสาเหตุของปัญหาที่เกิดขึ้นให้ท่านทราบถูกต้องมากน้อยเพียงใด	189	54	16	21	5
ท่านมีการเรียนรู้ ข้อผิดพลาดที่เกิดจากการใช้ระบบสารสนเทศ มากน้อยเพียงใด	23	58	125	34	45
รวม	411	220	306	141	62
% เฉลี่ยรวม	36.05	19.30	26.84	12.37	5.44

ภาพที่ 4.16

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 9 ด้านการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การ

(Information Security Incident Management)



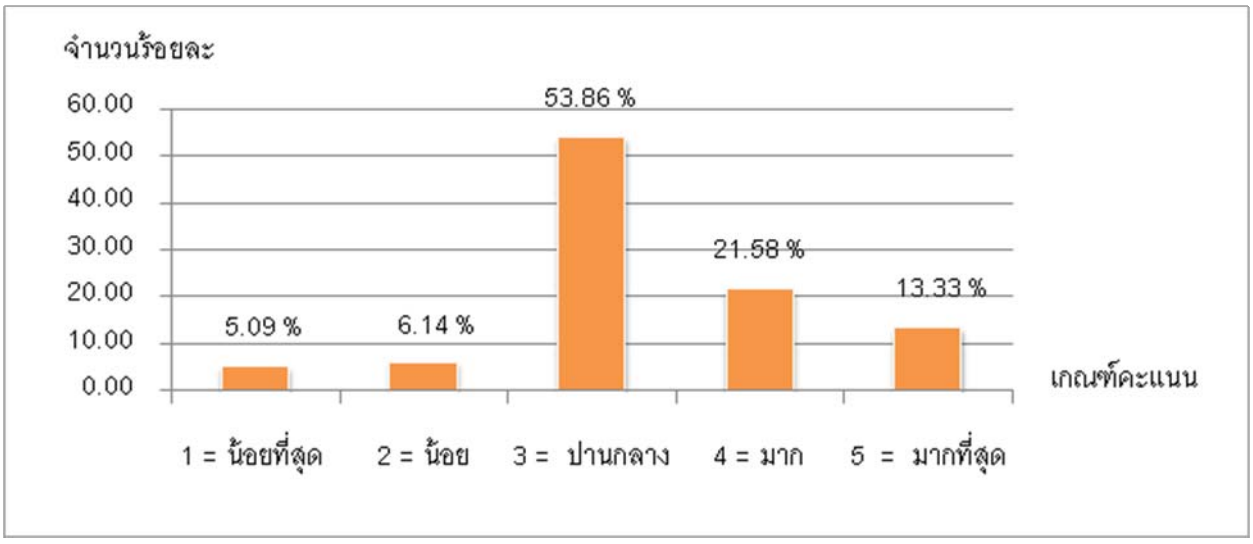
ตารางที่ 4.28

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 10 ด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์การ (Business Continuity Management)

ผลการสำรวจความคิดเห็นหมวดที่ 10	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเห็นว่าปัจจุบันการเจริญเติบโตทางด้านธุรกิจขององค์การมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์การมีมากน้อยเพียงใด	20	15	185	45	20
ท่านคิดว่าปัจจุบันองค์การมีแผนในการสร้างความต่อเนื่องของงานให้สามารถดำเนินงานได้ในระดับและช่วงเวลาที่กำหนดไว้ เหมาะสมมากน้อยเพียงใดหลังจากที่เกิดการติดขัด หยุดชะงัก หรือล้มเหลวของระบบ	9	20	122	78	56
รวม	29	35	307	123	76
% เฉลี่ยรวม	5.09	6.14	53.86	21.58	13.33

ภาพที่ 4.17

ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง หมวดที่ 10 ด้านการบริหารความต่อเนื่องในการดำเนินงานขององค์การ (Business Continuity Management)



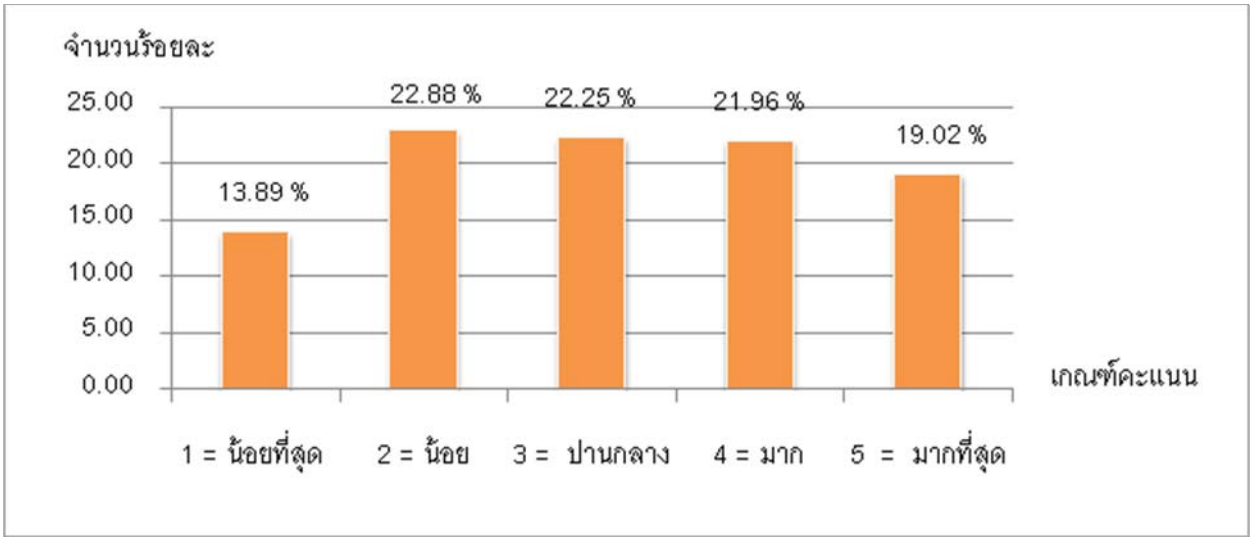
ตารางที่ 4.29

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

หมวดที่ 11 ด้านการปฏิบัติตามข้อกำหนด (Compliance)

ผลการสำรวจความคิดเห็นหมวดที่ 11	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเคยลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน๊ตบุ๊ก ขององค์การหรือไม่	56	40	78	99	12
ท่านเห็นว่าการเข้ารหัสข้อมูล เช่น การเข้าดูข้อมูล การผ่านเข้าออกในส่วนสำคัญต่างๆ ขององค์การ หรือการเข้าใช้งานอุปกรณ์ต่างๆ มีความเข้มงวดและปลอดภัยมากน้อยเพียงใด	35	58	78	52	62
ปัจจุบันผู้บังคับบัญชาคอยกำกับ ดูแลและควบคุมการปฏิบัติงานของท่าน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์การ มากน้อยเพียงใด	15	46	74	67	83
ท่านมีความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำเกี่ยวคอมพิวเตอร์ พ.ศ. 2550 มากน้อยเพียงใด	47	128	45	20	45
ท่านคิดว่าพนักงานภายในองค์การมีความตระหนักและให้ความสำคัญ กับปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำเกี่ยวคอมพิวเตอร์ พ.ศ. 2550 มากน้อยเพียงใด	45	54	42	75	69
รวม	198	326	317	313	271
% เฉลี่ยรวม	13.89	22.88	22.25	21.96	19.02

ภาพที่ 4.18
ร้อยละของความคิดเห็นของกลุ่มตัวอย่าง
หมวดที่ 11 ด้านการปฏิบัติตามข้อกำหนด (Compliance)



4. ผลสำรวจความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษาความปลอดภัยระบบสารสนเทศ

เป็นข้อมูลที่ได้จาก โดยใช้แบบสอบถาม เพื่อประเมินความเสี่ยงภายในองค์การ 3 ด้านคือ

1. ด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ
2. ด้าน Confidentiality - สิทธิในการเข้าถึงข้อมูลต่าง ๆ
3. ด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล

ซึ่งในการสำรวจเพื่อประเมินความเสี่ยงจะถูกแบ่งออกเป็น 2 ส่วนคือ

ส่วนที่ 1 สำหรับพนักงานทั่วไป ที่เกี่ยวข้องและเป็นผู้ใช้ระบบงานทางเทคโนโลยีสารสนเทศ โดยในกลุ่มนี้จะวิเคราะห์ เฉพาะด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ จำนวนกลุ่มตัวอย่างทั้งหมด 285 คน

ส่วนที่ 2 สำหรับเจ้าหน้าที่เทคโนโลยีสารสนเทศ โดยในกลุ่มนี้จะทำการวิเคราะห์ ความเสี่ยงทั้ง 3 ด้าน จำนวน 18 คน จากกลุ่มตัวอย่างทั้งหมด 285 คน

ผลของค่าเฉลี่ยความเสี่ยงที่ได้มาจากผลการคำนวณค่าเสี่ยงจากความคิดเห็นเรื่องโอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การและระดับความรุนแรงของความเสี่ยงขึ้นนั้นในองค์การของกลุ่มตัวอย่าง ตามสูตร

ระดับความเสี่ยง (R) = โอกาสเกิดภัยคุกคาม (L) x ความรุนแรงของผลกระทบ (I)

และนำระดับความเสี่ยงไปเปรียบเทียบค่าเพื่อจัดลำดับความเสี่ยงตามตาราง เมตริกซ์ระดับความเสี่ยง 5 x 5 ตารางที่ 4.30

โดยนำระดับความเสี่ยงที่ได้มาแบ่งกลุ่มระดับความเสี่ยงเป็นดังนี้

> 48.00 ความเสี่ยงสูง

= 16.01 – 48.00 ความเสี่ยงปานกลาง

$\leq$ 16.00 ความเสี่ยงต่ำ

ตารางที่ 4.30 เมตริกซ์ระดับความเสี่ยง 5 x 5

ระดับความรุนแรงของผลกระทบ	ระดับโอกาสในการเกิดเหตุการณ์				
	ประเภท 1 เกิดแน่นอนหรือสูงมาก = 1	ประเภท 2 แนวโน้มสูง = 0.8	ประเภท 3 ปานกลาง = 0.6	ประเภท 4 แนวโน้มต่ำ = 0.4	ประเภท 5 ต่ำมากหรือไม่เกิดเลย = 0.2
สูงมาก = 100	100 สูง	80 สูง	60 สูง	40 ปานกลาง	20 ปานกลาง
สูง = 80	80 สูง	60 สูง	48 ปานกลาง	32 ปานกลาง	16 ต่ำ
ปานกลาง = 60	60 สูง	48 ปานกลาง	36 ปานกลาง	24 ปานกลาง	12 ต่ำ
ต่ำ = 40	40 ปานกลาง	32 ปานกลาง	24 ปานกลาง	16 ต่ำ	8 ต่ำ
ต่ำมาก = 20	20 ปานกลาง	16 ต่ำ	12 ต่ำ	8 ต่ำ	4 ต่ำ

ตารางที่ 4.31
ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง
ความเสี่ยงด้าน Confidentiality

ด้าน Confidentiality – การรักษาความลับและสิทธิในการเข้าถึงข้อมูล	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
1. การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม	0.38	97.01	36.86	ปานกลาง
2. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน	0.72	81.40	58.61	สูง
3. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	0.91	86.21	78.45	สูง

<u>เหตุการณ์ที่ใช้ในการสำรวจความเสี่ยงด้าน Confidentiality มีทั้งหมด 3 เหตุการณ์ ดังนี้</u>

เหตุการณ์ที่ 1 การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม

<u>พฤติกรรม</u>

- ไม่มีการตั้งรหัสผ่าน (Password) ในการเข้าใช้ระบบ
- ในการตั้งรหัสผ่าน (Password) มีความง่ายจนเกินไป ทำให้ รหัสผ่าน (Password) ถูก ผู้ไม่ประสงค์ดีทำการไขรหัสได้โดยง่าย และเข้าสู่ระบบต่างๆ ได้
- มีการจดรหัสผ่าน (Password) ใส่กระดาษ แล้วนำไปไว้ในที่ที่จะสังเกตเห็นได้โดยง่าย

<u>ผลกระทบ</u>

มีความเสี่ยงในการเข้าใช้งานระบบจากผู้ที่ไม่ได้รับอนุญาต เนื่องจากสามารถเจาะผ่านเข้าระบบได้โดยง่าย

ผลการสำรวจ

การรักษารหัสผ่าน (Password) ของบุคคลอย่างไม่เหมาะสม มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.38 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 97.01 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 36.86 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 2 การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน

พฤติกรรม

ไม่มีการแยกหมวดหมู่ ในการเก็บข้อมูล โดยการเก็บข้อมูลที่สำคัญไว้ในฐานข้อมูลเดียวกัน

ผลกระทบ

มีโอกาสที่ข้อมูลจะสูญหายและโอกาสที่ข้อมูลทั้งหมดจะถูกผู้บุกรุกนำออกไปจากระบบค่อนข้างสูง เพราะผู้บุกรุกสามารถใช้ความพยายามในการเจาะระบบและขโมยข้อมูลเพียงที่ใดที่หนึ่งของระบบเท่านั้น เมื่อเจาะเข้ามาได้แล้วจะทำการแก้ไขดัดแปลงทำให้ข้อมูลเกิดความเสียหาย

ผลการสำรวจ

การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.72 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 81.40 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 58.61 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 3 การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล

พฤติกรรม

- มีการแอบใช้ชื่อหรือสิทธิของผู้อื่นโดยไม่ได้รับอนุญาต
- เจ้าของ User ID บอก User ID กับ รหัสผ่าน (Password) ให้กับบุคคลอื่นรับทราบ

ผลกระทบ

- ในกรณีที่มีการกระทำผิดกฎหมายตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเกิดเหตุขัดข้องกับระบบหรือข้อมูลภายในระบบ กระบวนการสืบหาผู้ที่เกี่ยวข้องหรือผู้กระทำผิดที่แท้จริงเป็นไปได้ยาก

- เกิดปัญหาทางด้านการถูกโจมตีระบบ และข้อมูลจากผู้ที่ไม่ประสงค์ดี เพราะ User ID จะถูกเผยแพร่ได้ง่าย ทำให้สามารถเข้าเครื่องคอมพิวเตอร์ด้วย User ID ของพนักงานคนใดคนหนึ่ง แล้วใช้เครื่องคอมพิวเตอร์เครื่องนั้นในการเข้าโจมตีระบบภายในองค์การ

ผลการสำรวจ

การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.91 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 86.21ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 78.45 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้วจะอยู่ใน ระดับสูง

สรุปผลการสำรวจความเสี่ยงด้าน Confidentiality

จากผลการสำรวจความเสี่ยงด้าน Confidentiality – การรักษาความลับและสิทธิในการเข้าถึงข้อมูล จากกลุ่มตัวอย่างทั้งหมด 285 คน พบว่าในด้านนี้จะมีความเสี่ยงสูง 2 เหตุการณ์คือ

1. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน
2. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล

ตารางที่ 4.32

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

ความเสี่ยงด้าน Availability (เฉพาะพนักงาน IT)

ด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
1. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้	0.85	80.25	68.21	สูง
2. การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป	0.36	64.29	23.14	ปานกลาง

ด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
3. การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง	0.47	70.59	33.18	ปานกลาง
4. ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย	0.33	42.86	14.14	ต่ำ
5. การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้	0.67	81.40	54.54	สูง
6. งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ	0.20	74.29	14.86	ต่ำ
7. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม	0.49	44.26	21.69	ปานกลาง
8. Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	0.22	71.43	15.72	ต่ำ
9. ข้อมูลที่เก็บสำรอง(Backup) ไม่เพียงพอ	0.67	75.68	50.71	สูง

<u>เหตุการณ์ที่ใช้ในการสำรวจความเสี่ยงด้าน Availability มีทั้งหมด 9 เหตุการณ์ ดังนี้</u>

เหตุการณ์ที่ 1 ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้

<u>พฤติกรรม</u>

การถูกเจาะระบบรักษาความปลอดภัยเข้ามายังเครื่อง Server ไม่ว่ากรณีใดๆ ก็ตาม

<u>ผลกระทบ</u>

ถ้าผู้บุกรุกสามารถเจาะระบบรักษาความปลอดภัยเข้ามายังเครื่อง Server ได้ ผู้บุกรุกอาจจะเข้ามาแก้ไขข้อมูล ทำให้เกิดการประมวลผลข้อมูลเกิดความผิดพลาด และนอกจากนี้ ผู้บุก

รุกอาจจะเข้ามาขัดจังหวะการทำงานของระบบ ทำให้ระบบสารสนเทศภายในองค์การ เกิดความเสียหาย จนถึงขั้นหยุดชะงัก

ผลสำรวจ

ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.85 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 80.25 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 68.21 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 2 การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป

พฤติกรรม

- การวางระบบการเชื่อมต่อเครือข่ายภายในองค์การ มีความซับซ้อนเกินไป
- การออกแบบระบบโปรแกรมที่ใช้งานมีความซับซ้อนจนเกินไป

ผลกระทบ

- สำหรับการวางระบบการเชื่อมต่อเครือข่ายภายในองค์การ ที่มีความซับซ้อนเกินไป จะส่งผลทำให้การติดต่อสื่อสารของระบบสารสนเทศภายในองค์การ เกิดความล่าช้า จนส่งผลให้เกิดการหยุดชะงักของระบบ และนอกจากนี้ การแก้ไขปัญหายังเกิดความล่าช้าอีกด้วย เนื่องจากระบบที่ซับซ้อนเกินไป

- การออกแบบระบบโปรแกรม (Application) ที่ใช้งานมีความซับซ้อนจนเกินไป จะส่งผลให้การประมวลผลข้อมูลช้า จนทำให้ไม่สามารถเข้าใช้งานระบบได้ตามต้องการ นอกจากนี้อาจจะเกิดความผิดพลาดของข้อมูลอีกด้วย

ผลสำรวจ

การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไปมีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.36 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 64.92 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 23.14 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 3 การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง

พฤติกรรม

- ติดตั้ง Server ไม่ถูกต้อง
- ติดตั้ง Software ไม่ครบและไม่ถูกวิธี

ผลกระทบ

ทำให้ระบบใช้งานไม่ได้ และอาจทำให้ข้อมูลเกิดความเสียหายไปด้วย

ผลสำรวจ

การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้องมีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.47 ซึ่งเป็นค่าอยู่ระดับปานกลาง และมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 70.59 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 33.18 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 4 ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย

พฤติกรรม

- มีการเรียกดูเว็บไซต์ของ www.thaipbs.or.th เป็นจำนวนมากเกินกว่าที่ได้คาดการณ์ไว้
- มีการเรียกใช้โปรแกรม (Application) ในช่วงเวลาใดเวลาหนึ่งมากเกินไป เกินกว่าที่ได้วางแผนรองรับไว้
- มีการใช้งานระบบเครือข่าย (Network) ในช่วงเวลาใดเวลาหนึ่งมากเกินไป เกินกว่าที่ระบบจะรองรับได้

ผลกระทบ

ทำให้ระบบล่ม

ผลสำรวจ

ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.33 ซึ่งเป็นค่าที่ต่ำ ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 42.86 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 14.14 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับต่ำ

เหตุการณ์ที่ 5 การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้

พฤติกรรม

- มีการบำรุงรักษาระบบ ในเวลาไม่เหมาะสม เช่น เวลาที่ยังมีการใช้งานระบบอยู่
- ไม่มีการแจ้งให้กับผู้ใช้ระบบทราบล่วงหน้าว่าจะมีการปิดระบบ
- ในกรณีที่มีการแจ้งแล้ว อาจจะแจ้งอย่างกระชั้นกระชิด ทำให้ผู้ใช้ระบบรับทราบไม่ทั่วถึง และไม่มีเวลาในเตรียมสำรองข้อมูล หรือดำเนินงานให้เสร็จไว้ล่วงหน้า เพื่อไม่ให้งานหยุดชะงัก

ผลกระทบ

ทำให้พนักงานไม่สามารถใช้งานระบบได้ ทำให้งานหยุดชะงักในระยะที่ไม่สมควร อาจจะจะส่งผลเสีย จากการที่ได้ข้อมูล หรือการดำเนินงานล่าช้า เนื่องจากการหยุดชะงักของระบบ

ผลสำรวจ

การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.67 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 81.40 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 54.54 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 6 งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ

พฤติกรรม

ไม่การตั้งงบประมาณในการจัดซื้อจัดหา ระบบสำรองข้อมูล (Backup) ภายในองค์กร

ผลกระทบ

- ไม่มีระบบสำรองข้อมูล (Backup) ทำให้เมื่อระบบใดระบบหนึ่งเกิดความเสียหาย ทำให้สูญเสียข้อมูลไปด้วย ซึ่งข้อมูลนั้น อาจเป็นข้อมูลที่สำคัญต่อการดำเนินงาน
- นอกจากนี้ การที่ไม่มีการสำรองข้อมูลไว้ เมื่อระบบเกิดความเสียหาย อาจจะส่งผลการใช้งานระบบ ที่ไม่สามารถใช้งานได้ เนื่องจากข้อมูลไม่มี

ผลสำรวจ

งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอมีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.20 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 74.29 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 14.86 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 7 พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม

พฤติกรรม

- เจ้าหน้าที่ IT ไม่มีการอบรมเกี่ยวความรู้ ความชำนาญเฉพาะด้าน ที่เกี่ยวกับการทำงานด้านเทคโนโลยีสารสนเทศ

ผลกระทบ

- เมื่อมีปัญหาใหม่ๆ เกิดขึ้น การแก้ไขปัญหาเป็นไปได้ช้า หรือบางครั้งอาจจะแก้ไขปัญหานั้นๆ ไม่ได้เลย เนื่องมากจากขาดความรู้ความชำนาญในเรื่องนั้นๆ

ผลสำรวจ

พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.49 ซึ่งเป็นค่าอยู่ระดับปานกลาง และมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 44.26 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 21.69 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 8 Router / Firewall เสียทำให้ไม่สามารถใช้งานได้

พฤติกรรม

อุปกรณ์ Router / Firewall เกิดปัญหาในการใช้งาน

ผลกระทบ

- อุปกรณ์ Firewall เป็นอุปกรณ์ที่เกี่ยวข้องกับระบบรักษาความปลอดภัยในการป้องกันผู้ที่ไม่ประสงค์ดีจากภายนอกเข้ามาขโมย ดัดแปลง แก้ไข ข้อมูลภายในองค์การ ถ้าอุปกรณ์ดังกล่าวทำให้ไม่มีระบบป้องกัน ทำให้ผู้ไม่ประสงค์ดีสามารถเข้ามา ดัดแปลง แก้ไข ข้อมูล ทำให้เกิดความเสียหายได้

- อุปกรณ์ Router เป็นอุปกรณ์ที่ใช้ระบบเชื่อมต่อ จากระบบหนึ่งไปยังระบบหนึ่ง ถ้าอุปกรณ์ดังกล่าวเกิดความเสียหาย จะส่งผลให้การให้บริการข้อมูลต่างๆ หยุดชะงัก ซึ่งถ้าเป็นข้อมูลสำคัญ จะส่งผลต่อการดำเนินงานภายในองค์กรเป็นอย่างมาก

ผลสำรวจ

Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.22 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 71.43 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 15.72 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 9 ข้อมูลที่เก็บสำรอง(Backup) ไม่เพียงพอ

พฤติกรรม

- ไม่มีการ Backup แบบ Full Backup
- ไม่มีการตรวจสอบผลสำเร็จการดำเนินงานในขั้นตอน
- ไม่มีการทดสอบการ Restore เพื่อตรวจสอบความครบถ้วนของข้อมูล

ผลกระทบ

ทำให้สูญเสียข้อมูล ในส่วนที่ไม่มีการ Backup ไว้

ผลสำรวจ

ข้อมูลที่เก็บสำรอง(Backup) ไม่เพียงพอ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.67 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 75.68 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 50.71 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้วจะอยู่ใน ระดับสูง

สรุปผลการสำรวจความเสี่ยงด้าน Availability

จากผลการสำรวจความเสี่ยงด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการจากกลุ่มตัวอย่างทั้งหมด 18 คน (เฉพาะเจ้าหน้าที่ IT) พบว่าในด้านนี้จะมีความเสี่ยงสูง 3 เรื่องคือ

1. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้
2. การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้
3. ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ

ตารางที่ 4.33
ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง
ความเสี่ยงด้าน Confidentiality (เฉพาะพนักงาน IT)

ด้าน Confidentiality - สิทธิในการเข้าถึงข้อมูลต่าง ๆ	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
1. การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง	0.65	77.38	50.30	สูง
2. การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง	0.38	78.57	29.86	ปานกลาง
3. การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง	0.63	82.19	51.78	สูง
4. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	0.69	70.97	49.97	สูง
5. การเข้าใช้ข้อมูลสำรอง (Backup) โดยปราศจากการควบคุม	0.24	51.43	12.34	ต่ำ

<u>เหตุการณ์ที่ใช้ในการสำรวจความเสี่ยงด้าน Confidentiality มีทั้งหมด 5 เหตุการณ์ ดังนี้</u>

เหตุการณ์ที่ 1 การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง

<u>พฤติกรรม</u>

- การเข้าใช้งานโปรแกรมประยุกต์เฉพาะจากผู้ที่ไม่เกี่ยวข้อง
- มีการเรียกดูรายงานที่สำคัญจากผู้ที่ไม่เกี่ยวข้อง

<u>ผลกระทบ</u>

1. ทำให้ข้อมูลสำคัญเกิดการรั่วไหล ส่งผลเสียต่อความมั่นคงขององค์การ

2. ในการเข้ามาใช้ระบบโดยผู้ไม่ประสงค์ อาจก่อให้เกิดความเสียหายต่อข้อมูล หรืออาจเข้ามาก่อกวนทำให้ระบบงานหยุดชะงักได้ และสามารถส่งผลเกี่ยวเนื่องไม่ยังระบบงานอื่นๆ อีกด้วย

ผลการสำรวจ

การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.65 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 77.38 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 50.30 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้วจะอยู่ใน ระดับสูง

เหตุการณ์ที่ 2 การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง

พฤติกรรม

เมื่อมีสร้างข้อมูลแล้วตั้งชื่อข้อมูลไม่ตรงกับข้อมูลจริงหรือกับการใช้งานจริง

ผลกระทบ

- เมื่อชื่อและข้อมูลไม่ตรงกับความเป็นจริง ทำให้เกิดปัญหาในการวิเคราะห์ เมื่อเกิดปัญหาขึ้น

- ส่งผลเมื่อต้องการนำข้อมูลกลับใช้ในระบบ เนื่องจากข้อมูลเดิมเกิดความเสีย ทำให้การนำข้อมูลกลับมาใช้ไม่ถูกต้อง ทำให้การประมวลผลผิดพลาด และการนำข้อมูลผิดไปใช้จะก่อให้เกิดความเสียต่อการดำเนินธุรกิจ

ผลการสำรวจ

การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.38 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 78.57 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 29.86 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ในระดับปานกลาง

เหตุการณ์ที่ 3 การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง

พฤติกรรม

ในการจัดเก็บข้อมูลไม่มีการแยกประเภทในการจัดเก็บ หรือจัดเก็บไม่ถูกประเภท ซึ่งเราจะแบ่งประเภทของข้อมูลเป็น 4 ประเภท คือ

1. ข้อมูลลับ (Secret Information)
2. ข้อมูลลับเฉพาะ (Confidential Information)
3. ข้อมูลที่จำเป็นมาก (Critical Information)
4. ข้อมูลสาธารณะหรือข้อมูลทั่วไป (General Information)

ผลกระทบ

ข้อมูลจะรั่วไหล ได้ง่าย เพราะถ้าข้อมูลที่เป็นข้อมูลลับ ถูกจัดไว้ในหมวดที่เป็นข้อมูลสาธารณะหรือข้อมูลทั่วๆไป ระบบการเข้าถึง และระบบการป้องกันจะมีขั้นตอนที่ไม่เหมือนกัน

ผลการสำรวจ

การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.63 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 82.19 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 51.78 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 4 การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม

พฤติกรรม

ไม่มีการควบคุมการพิมพ์เอกสาร ที่เป็นข้อมูลสำคัญออกนอกบริษัท

ผลกระทบ

- สูญเสียข้อมูลสำคัญ
- สูญเสียความน่าเชื่อถือ และความมั่นคงปลอดภัยภายในองค์การ

ผลการสำรวจ

การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.69 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 70.97 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่าเท่ากับ 49.97 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 5 การเข้าใช้ข้อมูลสำรอง (Backup) โดยปราศจากการควบคุม

พฤติกรรม

การสามารถเรียกดู หรือนำข้อมูลสำรองออกมาใช้งานโดยไม่ได้รับอนุญาต

ผลกระทบ

- สูญเสียข้อมูล และเกิดการรั่วไหลของข้อมูลความลับ
- ทำให้ระบบเกิดความเสียหาย เพราะการที่ผู้ไม่มีสิทธิ สามารถเข้าถึงข้อมูลอาจจะเข้ามาทำลายข้อมูล ทำให้เหมือนระบบเกิดความเสียหาย ผู้ดูแลระบบไม่สามารถกู้ข้อมูลคืนมาได้ เพราะข้อมูลดูทำลายไปแล้ว

- ทำให้การประมวลผลเกิดความผิดพลาด เพราะการที่ผู้ไม่มีสิทธิสามารถเข้าถึงข้อมูลได้ อาจจะเข้าดัดแปลงข้อมูลให้เกิดความเสียหายได้ เมื่อผู้ดูแลระบบนำข้อมูลสำรองกลับมาใช้ในระบบจริง ในกรณีที่ระบบจริงเกิดความเสียหาย จะเป็นการนำชุดข้อมูลที่ถูกแก้ไขโดยผู้ไม่มีสิทธิกลับมาใช้ในระบบจริง ทำให้เกิดความเสียหาย

ผลการสำรวจ

การเข้าใช้ข้อมูลสำรอง (Backup) โดยปราศจากการควบคุม มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.24 ซึ่งเป็นค่าที่ต่ำ และมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 51.43 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่าเท่ากับ 12.34 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้วจะอยู่ใน ระดับต่ำ

สรุปผลการสำรวจความเสี่ยงด้าน Confidentiality

จากผลการสำรวจความเสี่ยงด้าน Confidentiality - สิทธิในการเข้าถึงข้อมูลต่าง ๆ จากกลุ่มตัวอย่างทั้งหมด 18 คน (เฉพาะเจ้าหน้าที่ IT) พบว่าในด้านนี้จะมีความเสี่ยงสูง 3 เรื่องคือ

1. การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง
2. การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง
3. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม

ตารางที่ 4.34

ผลการสำรวจความคิดเห็นของกลุ่มตัวอย่าง

ความเสี่ยงด้าน Integrity (เฉพาะพนักงาน IT)

ด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
1. การเกิดความผิดพลาดในการรายงานผลข้อมูล	0.30	70.51	21.15	ปานกลาง
2. ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย	0.89	32.14	28.60	ปานกลาง

ด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล	โอกาสในการเกิด (Likelihood)	ระดับความรุนแรง (Impact)	ระดับความเสี่ยง = L x I	ระดับความเสี่ยงตารางเมตริกซ์ 5x5
3. ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และ ซอฟต์แวร์ทำงานผิดพลาด	0.56	91.95	51.49	สูง
4. การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบ สิทธิการใช้งานให้ทันสมัย	0.65	77.38	50.30	สูง
5. การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ	0.86	69.33	59.62	สูง
6. การขาดการเก็บบันทึกข้อมูลโปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง	0.86	73.68	63.36	สูง
7. มีการแก้ไขโปรแกรมประยุกต์ (Application) อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ	0.56	53.73	30.09	ปานกลาง
8. กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ	0.12	60.00	7.20	ต่ำ

เหตุการณ์ที่ใช้ในการสำรวจความเสี่ยงด้าน Integrity มีทั้งหมด 8 เหตุการณ์ ดังนี้

เหตุการณ์ที่ 1 การเกิดความผิดพลาดในการรายงานผลข้อมูล

พฤติกรรม

การประมวลผลข้อมูลในระบบผิดพลาด เช่น อาจจะมาจากการเขียนโปรแกรมที่ซับซ้อน หรือ เขียนโปรแกรมไม่ถูกต้อง

ผลกระทบ

ทำให้เกิดปัญหาต่อผู้นำข้อมูลไปใช้

ผลการสำรวจ

การเกิดความผิดพลาดในการรายงานผลข้อมูล มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.30 ซึ่งเป็นค่าที่ต่ำ แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 70.51 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่า = 21.15 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 2 ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย

พฤติกรรม

- ไม่มีการอัพเดทข้อมูลต่างๆ เช่น ข้อมูลผู้ใช้งาน , ข้อมูลรายละเอียดเครื่อง Server , ข้อมูลการเข้าใช้งานอินเตอร์เน็ต ให้เป็นปัจจุบัน

ผลกระทบ

เมื่อไม่มีการอัพเดทข้อมูลที่เป็นปัจจุบัน ทำให้การวิเคราะห์ข้อมูลเกิดความผิดพลาด และการนำข้อมูลไปใช้ผิด

ผลการสำรวจ

ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.89 ซึ่งเป็นค่าที่สูง แต่เนื่องจากค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่า 32.14 ซึ่งอยู่ในระดับปานกลาง ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจะมีค่า = 28.60 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับปานกลาง

เหตุการณ์ที่ 3 ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด

พฤติกรรม

การที่ Server เกิดขัดข้องทำให้ฐานข้อมูลบนเครื่อง ดังกล่าวหยุดทำงานชั่วขณะ ทำให้ข้อมูลในช่วงเวลาดังกล่าวไม่ถูกเก็บลงฐานข้อมูล

ผลกระทบ

- สูญเสียข้อมูลในช่วงที่เกิดความขัดข้องกับฮาร์ดแวร์และซอฟต์แวร์ ซึ่งอาจจะเป็นช่วงของข้อมูลที่สำคัญ
- ทำให้ระบบที่เกี่ยวข้องต้องเกิดการหยุดชะงัก

ผลการสำรวจ

ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.56 และค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 91.95 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 51.49 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 4 การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบ สิทธิการใช้งานให้ทันสมัย

พฤติกรรม

- ไม่มีการพัฒนาระบบรักษาความปลอดภัยที่ต่อเนื่อง และมีประสิทธิภาพเพียงพอ
- ยังไม่มีระบบตรวจสอบผลการดำเนินงานทางด้านระบบรักษาความปลอดภัย

ผลกระทบ

ระบบมีความเสี่ยงในการถูกโจมตี

ผลการสำรวจ

การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบ สิทธิการใช้งานให้ทันสมัย มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.65 และค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 77.38 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 50.30 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 5 การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ

พฤติกรรม

ไม่มีกระบวนการตรวจสอบภายใน

ผลกระทบ

ทำให้ควบคุมการใช้งานข้อมูลเป็นไปอย่างลำบาก

ผลการสำรวจ

การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.86 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 69.33 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 59.62 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 6 การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง

พฤติกรรม

หลังจากที่มีการแก้ไข โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ไม่มีการบันทึกการเปลี่ยนแปลงเป็นลายลักษณ์อักษร

ผลกระทบ

เมื่อโปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) เกิดปัญหาขึ้น ทำให้ยากต่อการแก้ไข เพราะจะไม่สามารถว่าได้แก้ไขตรงจุดไหนไปบ้าง

ผลการสำรวจ

การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.86 ซึ่งเป็นค่าที่สูง ประกอบกับมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบมีค่าสูงถึง 73.68 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 63.36 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 7 มีการแก้ไขโปรแกรมประยุกต์ (Application) อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ

พฤติกรรม

เมื่อมีการแก้ไขโปรแกรมประยุกต์ (Application) ไม่มีการทดสอบก่อนนำไปใช้จริง

ผลกระทบ

ในกรณีที่มีการแก้ไขโปรแกรมประยุกต์ (Application) แล้วไม่มีการทดสอบก่อน นำขึ้นระบบที่ใช้งานจริงเลย ในกรณีที่การแก้ไขมีปัญหาเกิด จะส่งผลให้ระบบที่ใช้จริงอยู่หยุดชะงักได้

ผลการสำรวจ

มีการแก้ไขโปรแกรมประยุกต์ (Application) อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.56 และมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 53.73 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 30.09 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับสูง

เหตุการณ์ที่ 8 กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ

พฤติกรรม

กระบวนการในการเข้าใช้งานระบบ มีความซับซ้อนจนเกินไป ทำให้ผู้ใช้งานไม่มีความเข้าใจ

ผลกระทบ

เมื่อผู้ใช้งานไม่มีความเข้าใจในการเข้าใช้ระบบ ทำให้ผู้ใช้มีขั้นตอน หรือเรียกใช้ระบบผิดวิธี ทำให้เกิดปัญหาในการประมวลผลข้อมูลได้

ผลการสำรวจ

กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ มีค่าเฉลี่ยโอกาสการเกิดอยู่ที่ 0.12 และมีค่าเฉลี่ยระดับความรุนแรงของผลกระทบอยู่ที่ 60.00 ทำให้เมื่อทำการคำนวณหาค่าระดับความเสี่ยงจึงมีค่า = 7.20 เมื่อนำไปเทียบกับตารางเมตริกซ์ 5x5 แล้ว จะอยู่ใน ระดับต่ำ

สรุปผลการสำรวจความเสี่ยงด้าน Integrity

จากผลการสำรวจความเสี่ยงด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล จากกลุ่มตัวอย่างทั้งหมด 18 คน (เฉพาะเจ้าหน้าที่ IT) พบว่าในด้านนี้จะมีความเสี่ยงสูง 4 เรื่อง โดยเรียงลำดับความเสี่ยงจากมากไปน้อย

1. การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง
2. การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ
3. ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน
4. การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบ สิทธิการใช้งานให้ทันสมัย

ผลการวิเคราะห์ความสัมพันธ์ระหว่างความเสี่ยง กับมาตรฐาน ISO/IEC 27001

จากการสำรวจและการประเมินความเสี่ยงทั้ง 3 ด้านจากกลุ่มตัวอย่างพนักงานในองค์การที่เกี่ยวข้องมาแล้วนั้นมีทั้ง 12 เหตุการณ์ที่จัดเป็นความเสี่ยงสูงที่เกิดขึ้นภายในองค์การ คือ

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

ตารางที่ 4.35

ตารางแสดงความสัมพันธ์ระหว่างความเสี่ยง กับมาตรฐาน ISO/IEC 27001

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
1. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	กำลังดำเนินจัดทำนโยบายทางด้านความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบ ว่าองค์การมีการจัดทำนโยบายทางด้านความมั่นคงปลอดภัย
	หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน และในระหว่างการ จ้างงาน	- ไม่มีการกระบวนลงโทษทางวินัยสำหรับผู้ที่ทำผิดนโยบาย	กลุ่มตัวอย่างร้อยละ 42.11 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด
2. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	กำลังดำเนินจัดทำนโยบายทางด้านความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบ ว่าองค์การมีการจัดทำนโยบายทางด้านความมั่นคงปลอดภัย
	หมวดที่ 7 ด้านการควบคุมการเข้าถึง	- ไม่มีนโยบายควบคุมการเข้าใช้ระบบ - ไม่มีนโยบายการใช้บริการเครือข่าย - ไม่มีการจำกัดระยะเวลาในการเชื่อมต่อเข้าระบบ	กลุ่มตัวอย่างร้อยละ 27.28 เห็นว่าการดำเนินงานตามหมวดที่ 7 ยังอยู่ระดับน้อย ซึ่งเป็นความเห็นส่วนใหญ่ของกลุ่มตัวอย่าง

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
		สารสนเทศ - ไม่มีการแยกระบบสารสนเทศที่มีความสำคัญออกจากระบบทั่วไป	
3. การขาดการเก็บบันทึกข้อมูลโปรแกรมประยุกต์ (Application) ระบบ (System) หรือซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง	หมวดที่ 6 ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร	- ไม่มีการจัดทำ หรือออกระเบียบเกี่ยวกับการเปลี่ยนแปลง ปรับปรุงแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ	กลุ่มตัวอย่างร้อยละ 35.31 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด ซึ่งเป็นความเห็นส่วนใหญ่ของกลุ่มตัวอย่าง
4. การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	นโยบายในการบริหารจัดการ ที่เป็นลายลักษณ์ในปัจจุบันยังไม่สมบูรณ์	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบ ว่าองค์การมีการจัดทำนโยบายทางด้านความมั่นคงปลอดภัย
	หมวดที่ 2 ด้านโครงสร้างทางด้านความมั่งคงปลอดภัยภายในองค์การ และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก	ไม่มีการทบทวนทางด้านความมั่นคงปลอดภัยจากผู้ตรวจสอบอิสระ	กลุ่มตัวอย่างร้อยละ 43.68 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
5. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	กำลังดำเนินจัดทำนโยบายทางด้านความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบนโยบายทางด้านความมั่นคงปลอดภัย
	หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการ จ้างงาน (During employment)	องค์การยังมีการอบรมให้ความรู้ ให้กับพนักงาน	กลุ่มตัวอย่างร้อยละ 42.11 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด
6. การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	ยังไม่มีการระบุข้อกำหนด เกี่ยวกับการขั้นตอนปฏิบัติในการที่จะการดูแลรักษา (Maintenance) ไว้ในนโยบายความมั่นคงปลอดภัย	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบนโยบายทางด้านความมั่นคงปลอดภัย
	หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	- ไม่มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงและแก้ไขระบบ	กลุ่มตัวอย่างร้อยละ 53.33 มีความเห็นว่าการดำเนินงานตามหมวดที่ 8 ยังอยู่ในระดับที่น้อย

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
7. การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง	หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน และในระหว่างการ จ้างงาน	องค์การยังมีการอบรมให้ความรู้ทางด้านเทคโนโลยีสารสนเทศแก่พนักงานไม่สม่ำเสมอ และยังอยู่ในเกณฑ์น้อย	กลุ่มตัวอย่างร้อยละ 42.11 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด
8. ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟต์แวร์ทำงานผิดพลาด	หมวดที่ 8 ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	- ไม่มีการควบคุมการติดตั้ง Software ไปยังระบบที่ให้บริการ - ไม่มีการตรวจสอบการทำงานของ Software ภายหลังจากที่มีการแก้ไขระบบปฏิบัติการ	กลุ่มตัวอย่างร้อยละ 53.33 มีความเห็นว่าการดำเนินงานตามหมวดที่ 8 ยังอยู่ในระดับที่น้อย
9. การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง	หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน และในระหว่างการ จ้างงาน	- ไม่มีการถอดสิทธิในการเข้าใช้งาน สำหรับผู้ใช้งานที่สิ้นสุดการจ้างงานไปแล้ว	กลุ่มตัวอย่างร้อยละ 42.11 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด
10. ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ	หมวดที่ 6 ด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร	- ไม่มีการสำรอง และทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ	กลุ่มตัวอย่างร้อยละ 35.31 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด ซึ่งเป็นความเห็นส่วนใหญ่ของกลุ่มตัวอย่าง

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
11. การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานให้ทันสมัย	หมวดที่ 1 ด้านนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	นโยบายทางด้านความมั่นคงปลอดภัย ที่เป็นลายลักษณ์อักษร ยังไม่สมบูรณ์	กลุ่มตัวอย่างร้อยละ 87.84 ไม่ทราบนโยบายทางด้านความมั่นคงปลอดภัย
12. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	หมวดที่ 2 ด้านโครงสร้างทางด้านความมั่งคงปลอดภัยภายในองค์การ และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก	- ไม่มีการให้พนักงาน ลงนามมิให้เปิดเผยความลับ	กลุ่มตัวอย่างร้อยละ 43.68 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด
	หมวดที่ 4 ด้านการสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน และในระหว่างการ จ้างงาน	- ไม่มีการอบรมให้กับพนักงานได้ตระหนัก ให้ความรู้ และการอบรมด้านความปลอดภัย เช่น การอมรมเพื่อสร้างความเข้าใจให้ตรงกันทั้งในการจัดเก็บ การรักษา การนำไปใช้ การจัดพิมพ์ เป็นต้น - ไม่มีบทลงโทษสำหรับผู้ที่ทำการเผยแพร่ข้อมูลสำคัญ	กลุ่มตัวอย่างร้อยละ 42.11 เห็นว่าการดำเนินงานตามหมวดที่ 4 ยังอยู่ระดับน้อยที่สุด

เหตุการณ์ความเสี่ยง	มาตรฐาน ISO/IEC 27001		
	หมวดที่เกี่ยวข้อง	สถานะการดำเนินงาน (ข้อมูลได้จากการสัมภาษณ์)	ผลสำรวจ (ข้อมูลได้จากกลุ่มตัวอย่าง)
	หมวดที่ 7 ด้านการควบคุมการเข้าถึง	- ไม่มีการจัดทำนโยบายควบคุมการเข้าถึงระบบ เช่น การบริหารจัดการการเข้าถึงของผู้ใช้ การควบคุมการพิมพ์เอกสาร เป็นต้น	กลุ่มตัวอย่างร้อยละ 27.28 เห็นว่าการดำเนินงานตามหมวดที่ 7 ยังอยู่ระดับน้อย ซึ่งเป็นความเห็นส่วนใหญ่ของกลุ่มตัวอย่าง

<u>สรุปผลการวิเคราะห์ความสัมพันธ์</u>

จากการวิเคราะห์ความสัมพันธ์ระหว่างความเสี่ยง กับมาตรฐาน ISO/IEC27001 จะเห็นว่าการที่องค์กรไม่มีการปฏิบัติตามกรอบของ ISO/IEC 27001 จะทำให้มีความเสี่ยงเกิดขึ้นภายในองค์การ