ภาคผนวก

ข. ตัวอย่างแบบสอบถาม

แบบสอบถาม

สำหรับงานวิจัยเรื่อง

" การสร้างมาตรการทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ในอุตสาหกรรมวิทยุโทรทัศน์

โดยนำมาตรฐาน ISO/IEC 27001 มาประยุกต์ใช้

และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 "

วัตถุประสงค์

1. เพื่อหาแนวทางในการกำหนดนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศภายในองค์การ โดยใช้แนวคิดตามกรอบของ ISO/IEC27001 และให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2551

2. เพื่อหาแนวทางในการปฏิบัติงานในองค์การที่เหมาะสมในการใช้เครือข่ายสารสนเทศ เพื่อลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นต่อข้อมูลภายในองค์การ ทั้งนี้ เพื่อช่วยเพิ่มความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ

คำชี้แจง

แบบสอบถาม แบ่งออกเป็น 3 ส่วนได้แก่

ส่วนที่ 1 ข้อมูลทั่วไป

ส่วนที่ 2 คำถามข้อมูลในการแสดงความคิดเห็น ด้านการรักษาความปลอดภัยของระบบสารสนเทศ (โดยในที่นี่จะระบบสารสนเทศ ประกอบไปด้วย ข้อมูล ระบบคอมพิวเตอร์และเครือข่ายภายในองค์การ)

ส่วนที่ 3 คำถามข้อมูลในการแสดงความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษาความปลอดภัยในองค์การ (คำถามเฉพาะพนักงานที่มีหน้าที่ดูแลทางด้านระบบสารสนเทศ IT)

ส่วนที่ 1 : ข้อมูลทั่วไป

1.1 เพศ

☐ ชาย ☐ หญิง

1.2 อายุ

☐ < 20 ปี ☐ 21 – 25 ปี ☐ 26 – 30 ปี ☐ 31 – 35 ปี ☐ 36 – 40 ปี

☐ 41 – 45 ปี ☐ 46 – 50 ปี ☐ 51 – 55 ปี ☐ > 56 ปี

1.3 วุฒิการศึกษา

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ ปริญญาโท ☐ ปริญญาเอก

1.4 ประสบการณ์ทำงาน

☐ < 1 ปี ☐ 1 - 2 ปี ☐ 3 – 4 ปี ☐ 5 – 10 ปี ☐ > 10 ปี

1.5 ระยะเวลาในการทำงานที่องค์การปัจจุบัน

☐ < 1เดือน ☐ 1 - 4 เดือน ☐ 5 – 8 เดือน ☐ 9 – 12 เดือน ☐ > 1 ปี

1.6 ตำแหน่งงานในองค์การ

☐ ระดับปฏิบัติการ ☐ ระดับหัวหน้าส่วนงาน/ผู้จัดการ ☐ รองผู้อำนวยการ / ผู้อำนวยการ

1.7 หน่วยงานที่สังกัดในองค์การ

☐ ฝ่ายข่าว ☐ ฝ่ายรายการ ☐ ฝ่ายวิศวกรรม ☐ ฝ่ายผลิตรายการ

☐ ฝ่ายเทคโนโลยีสารสนเทศ ☐ สำนักบริหาร ☐ สำนักการคลัง

☐ สถาบันวิชาการสื่อสาธารณะ ☐ สำนักทรัพยากรมนุษย์ ☐ E-Radio และ Website

☐ สื่อประชาสังคม ☐ สำนักส่งเสริมการมีส่วนร่วม ☐ สำนักการตลาดเพื่อสังคม

ส่วนที่ 2 ข้อมูลในการแสดงความคิดเห็น ด้านการรักษาความปลอดภัยระบบสารสนเทศภายในองค์การ

คำถามด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านทราบหรือไม่ว่าปัจจุบันองค์การมีการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร (กรณีที่ไม่ทราบ ข้ามไปทำข้อ 2) (1 = ไม่ทราบ , 5 = ทราบ)					
ท่านทราบรายละเอียดของนโยบายดังกล่าวหรือไม่ (1 = ไม่ทราบ , 5 = ทราบ)					
ท่านทราบแหล่งที่สามารถเข้าไปอ่านนโยบายดังกล่าวหรือไม่ (1=ไม่ทราบ, 5=ทราบ)					

คำถามด้าน โครงสร้างทางด้านความมั่งคงปลอดภัยภายในองค์การ (Internal Organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านทราบหน้าที่ความรับผิดชอบของท่านในการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยเพียงใด					
ท่านคิดว่ากระบวนการขอใช้อุปกรณ์ประมวลผลสารสนเทศ มีขั้นตอนที่เหมาะสมหรือไม่					
ท่านทราบเรื่องการรักษาและไม่เปิดเผยความลับขององค์การมากน้อยเพียงใด					
ท่านคิดว่าผู้บริหารองค์การ ให้ความสำคัญกับการบริหารจัดการด้านความมั่นคงปลอดภัยทางด้านระบบสารสนเทศภายในองค์การมากน้อยเพียงใด					

คำถามด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์การ (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าองค์การมีการระบุความเป็นเจ้าของในอุปกรณ์สารสนเทศ อย่างชัดเจนและเหมาะสมหรือไม่					
ท่านทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์การ สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศมากน้อยแค่ไหน					
ท่านสามารถแบ่งประเภทของข้อมูลได้มากน้อยแค่ไหน เช่น ข้อมูลลับ(Secret Information),ข้อมูลลับเฉพาะ(Confidential Information),ข้อมูลที่จำเป็นมาก(Critical Information),ข้อมูลสาธารณะหรือข้อมูล					

คำถามด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application)ต่างๆ ภายในองค์การมีความเหมาะสมเพียงใดในปัจจุบัน					
ท่านเคยได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยแค่ไหน					
ท่านคิดว่าคุณสมบัติของผู้ให้บริการทางด้านสารสนเทศมีความรู้ความสามารถ เหมาะสมกับงานมากน้อยแค่ไหน					
ท่านทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายระเบียบปฏิบัติทางด้านความปลอดภัยขององค์การมากน้อยแค่ไหน					

คำถามด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่ากระบวนการคืนทรัพย์สินขององค์การ มีความเหมาะสมและครบถ้วนมากน้อยเพียงใด					
ท่านคิดว่ามาตรการในการถอดสิทธิ์การเข้าใช้งาน ระบบและโปรแกรมประยุกต์(Application)ต่างๆ สำหรับพนักงานลาออกไปแล้ว อยู่ในระดับที่เหมาะสมเพียงใด					

คำถามด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าปัจจุบันบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศขององค์การที่สำคัญ มีความเหมาะสมหรือความปลอดภัยมากน้อยเพียงใด					
ท่านคิดว่าการจัดทำบริเวณ ล้อมรอบ การเข้าถึงอุปกรณ์สารสารเทศ ภายในองค์การมีความเหมาะสมเพียงใด เช่น การควบคุมการเข้า - ออกของสำนักงาน					
ท่านคิดว่าการควบคุมการเข้า - ออก บริเวณพื้นที่สำคัญหรือที่ต้องการรักษาควมปลอดภัยมีความเหมาะสมหรือปลอดภัยมากน้อยเพียงใด					
ท่านมีการระวังและป้องกันอุบัติเหตต่างๆ มากน้อยเพียงใด เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชน หรือ เสี่ยงต่อการเกิดเข้าใช้งานจากผู้ไม่มีสิทธิเป็นต้น					
ท่าคิดว่าองค์กรมีการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานมากน้อยเพียงใด					

คำถามด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communication and Operations Management)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
หน่วยงานของท่านมีการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented Operating Procedures) ตามระยะเวลาอันสมควรสม่ำเสมอมากน้อยเพียงใด					
ท่านเห็นว่าองค์กรมีการบริหารจัดการเครือข่าย (Network Control) และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบ และโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายมีเหมาะสมเพียงใด					
ท่านให้ความสำคัญในการจัดเก็บเอกสารหรือข้อมูลต่างๆ ในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต หรือไม่เกี่ยวข้องมากน้อยเพียงใด					
ท่านทราบกฎระเบียบ ข้อบังคับ สิทธิของการส่งข้อมูลต่างๆ ออกไปนอกองค์กรมากน้อยเพียงใด					
ท่านทราบกฎระเบียบ ข้อบังคับ สิทธิของการใช้อินเตอร์เน็ตขององค์กรมากน้อยเพียงใด					
ท่านทราบกฎระเบียบ ข้อบังคับ สิทธิของการใช้อีเมล์ขององค์กรมากน้อยเพียงใด					
ท่านเห็นว่าองค์กรมีการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT สม่ำเสมอมากน้อยเพียงใด					
ท่านคิดว่าเครื่องคอมพิวเตอร์ภายในองค์การ มีการตั้งเวลาได้ถูกต้อง แม่นยำ มากน้อยแค่ไหน					

คำถามด้าน การควบคุมการเข้าถึง (Access Control)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์กรมากน้อยเพียงใด					
ถ้าองค์กรมีการแจ้ง หรือสรุป สิทธิการใช้งานระบบหรือโปรแกรมต่างๆ ภายในองค์กร ให้ท่านทราบตามระยะที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) ท่านเห็นด้วยมากน้อยเพียงใด					
ท่านให้ความสำคัญกับการ Log Off เครื่อง หรือปิดเครื่อง เมื่อท่านไม่อยู่เป็นเวลานาน เช่น ประชุม , ทานอาหารกลางวัน มากน้อยเพียงใด					
ท่านให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ท่านใช้งานมากน้อยเพียงใด					
ท่านให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆ ขององค์กรมากน้อยเพียงใด					

คำถามด้าน การควบคุมการเข้าถึง (Access Control) ต่อ	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเห็นว่ามาตรฐานการใส่ User ID & Password ก่อนเข้าใช้งานระบบต่างๆ ภายในองค์กร (ระบบบริหารจัดการรหัสผ่าน - Password Management System) มีความเหมาะสมและปลอดภัยมากน้อยเพียงใด					
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆ ขององค์การมากน้อยเพียงใด เช่น โปรแกรม Photoshop , ACDSee หรือโปรแกรมอื่นๆ ที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์					
ท่านมีการตรวจสอบอุปกรณ์ต่อพ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์การมากน้อยเพียงใด ตัวอย่าง การ Scan ไวรัสใน HandDrive ก่อนใช้งาน ฯลฯ					

คำถามด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition , Development and Maintenance)	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 %)					
ท่านเคยประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนบ้างหรือไม่และมากน้อยเพียงใด (1 =ไม่เคย 0% , 2 = พบประมาณ 1 - 25 % , 3 = พบประมาณ 26 - 50 % , 4 = พบประมาณ 51 - 75 % , 5 = พบประมาณ 76 - 100 %)					
ท่านเคยประสบปัญหาต่างๆ ดังกล่าวท่านได้ทำการแจ้งทีมงานผู้ดูแลผ่านช่องทางที่กำหนดหรือไม่ กรณีผู้ที่ไม่เคยประสบปัญหาใดๆ การใช้งานขอให้ข้ามไปข้อต่อไป (1 =ไม่เคยแจ้ง , 3 = แจ้ง แต่ไม่ทุกครั้ง , 5 = แจ้งทุกครั้งที่พบ)					

คำถามด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การ (Information Security Incident Management)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านคิดว่าซอฟต์แวร์ป้องกันไวรัสและมาตรการต่างๆ ในการป้องกันไวรัสขององค์การมีความเหมาะสมมากน้อยเพียงใด					
ท่านเคยรายงานเหตุการณ์หรือรายงานจุดอ่อน จุดบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์การที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่มากน้อยเพียงใด					
ท่านคิดว่า ทางส่วนงานเทคโนโลยีสารสนเทศ การรายงานถึงข้อผิดพลาด และสาเหตุของปัญหาที่เกิดขึ้นให้ท่านทราบถูกต้องมากน้อยเพียงใด					
ท่านมีการเรียนรู้ ข้อผิดพลาดที่เกิดจากการใช้ระบบสารสนเทศ มากน้อยเพียงใด					

คำถามด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์การ (Business Continuity Management)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเห็นว่าปัจจุบันการเจริญเติบโตทางด้านธุรกิจขององค์การมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์การมีมากน้อยเพียงใด					
ท่านคิดว่าปัจจุบันองค์การมีแผนในการสร้างความต่อเนื่องของงานให้สามารถดำเนินงานได้ในระดับและช่วงเวลาที่กำหนดไว้ เหมาะสมมากน้อยเพียงใด หลังจากที่เกิดการติดขัด หยุดชะงัก หรือล้มเหลวของระบบ					

คำถามด้าน การปฏิบัติตามข้อกำหนด (Compliance)	1 น้อยที่สุด	2 น้อย	3 ปานกลาง	4 มาก	5 มากที่สุด
ท่านเคยลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน๊ตบุ๊ก ขององค์การหรือไม่					
ท่านเห็นว่าการเข้ารหัสข้อมูล เช่น การเข้าดูข้อมูล การผ่านเข้าออกในส่วนสำคัญต่างๆ ขององค์การ หรือการเข้าใช้งานอุปกรณ์ต่างๆ มีความเข้มงวดและปลอดภัยมากน้อยเพียงใด					
ปัจจุบันผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของท่าน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์การ มากน้อยเพียงใด					
ท่านมีความรู้ความเข้าใจเกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำเกี่ยวคอมพิวเตอร์ พ.ศ. 2550 มากน้อยเพียงใด					
ท่านคิดว่าพนักงานภายในองค์การมีความตระหนักและให้ความสำคัญ กับปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำเกี่ยวคอมพิวเตอร์ พ.ศ. 2550 มากน้อยเพียงใด					

การระบุด้านความเสี่ยง					
คำถามด้าน Confidentality - สิทธิในการเข้าถึงข้อมูลต่างๆ	1 ไม่เกิด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด
1. การรักษารหัสผ่าน (Password) บองบุคคลอย่างไม่เหมาะสม เช่น การจดรหัสผ่านติดไว้ที่หน้าจอ การตั้งรหัสผ่านเป็นชื่อ - นามสกุลของตัวเอง เป็นต้น					
โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					
ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ					
2. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกัน เช่น เก็บข้อมูลสำคัญของแผนกไว้ใน Database เดียวกันหมด ซึ่งเสี่ยงเมื่อเกิดความเสียหายต่อ Database เครื่องดังกล่าว					
โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					
ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ					
3. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล หมายถึง การใช้ชื่อหรือสิทธิของผู้อื่นไม่ว่าจะได้รับอนุญาตจากเจ้าของหรือไม่ก็ตาม ในการเข้าใช้ข้อมูลที่ต้องมีการตรวจสอบสิทธิและการพิสูจน์ตัวตน					
โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					
ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ					

ท่านเคยพบปัญหาเรื่องการใช้งานระบบภายในองค์การด้านใดบ้าง

_____

_____

_____

ส่วนที่ 3 ข้อมูลการแสดงความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยทางด้านข้อมูลสารสนเทศในองค์การ (เฉพาะพนักงานที่มีหน้าที่ดูแลระบบสารสนเทศ IT)

การระบุด้านความเสี่ยง										
คำถามด้าน Confidentiality - สิทธิในการเข้าถึงข้อมูลต่าง ๆ	โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ				
	1 ไม่เกิด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด	1 ต่ำสุด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด
1. การเข้าถึงข้อมูลจากที่ไม่มีสิทธิใช้งานจริง เช่น การเข้าใช้งานโปรแกรมประยุกต์เฉพาะจากผู้ที่ไม่เกี่ยวข้อง การสามารถเรียกดูรายงานที่สำคัญจากผู้ที่ไม่เกี่ยวข้อง										
2. การระบุชื่อข้อมูลที่สร้างไม่ถูกต้อง หมายถึง มีการสร้างข้อมูลแล้วตั้งชื่อข้อมูลไม่ตรงกับข้อมู,จริงหรือการใช้งาน เช่น ข้อมูลที่ตั้งชื่อขึ้นต้นด้วยวันที่ที่สร้างข้อมูล เพื่อใช้ในการวิเคราะห์ปัญหา ถูกตั้งชื่อวันที่ผิด										
3. การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง หมายถึง การไม่สามารถจัดประเภทข้อมูลที่เป็น ข้อมูลลับ (Secret Informaion) , ข้อมูลลับเฉพาะ (Confident Information) , ข้อมูลที่จำเป็นมาก (Critical Information) , ข้อมูลสาธารณะหรือข้อมูลทั่วไป จึงอาจเกิดการจัดเก็บหรือรักษา ที่ไม่ถูกต้อง เช่น เก็บข้อมูลทดสอบไว้บนเครื่อง Server ที่ใช้งานจริง										
4. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม เช่น การพิมพ์ข้อมูลความลับขององค์กรออกนอกบริษัท										
5. การเข้าใช้ข้อมูลสำรอง (Backup) โดยปราศจากการควบคุม หมายถึง การสามารถเรียกดู หรือ นำข้อมูลสำรองออกมาใช้งานโดยไม่ได้รับอนุญาต										

คำถามด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล	โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ				
	1 ไม่เกิด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด	1 ต่ำสุด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด
1. การเกิดความผิดพลาดในการรายงานผลข้อมูล เช่น การประมวลผลข้อมูลในระบบผิดพลาด ดังนั้น เมื่อผู้ใช้งานนำข้อมูลออกจากระบบไปใช้ ทำให้เกิดปัญหาต่อผู้ใช้ข้อมูล										
2. ข้อมูลภายในองค์การขาดการพัฒนาหรืออัพเดท (Update) ให้ทันสมัย										
3. ฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และ ซอฟต์แวร์ทำงานผิดพลาด หมายถึง การที่เครื่อง Server เกิดขัดข้องทำให้ Database บนเครื่อง Server ดังกล่าว หยุดการทำงาน ชั่วขณะ ทำให้ข้อมูลในช่วงเวลาดังกล่าวไม่ถูกเก็บลง Database และทำให้การ ทำงานที่เกี่ยวข้องต้องหยุดตาม										
4. การขาดการพัฒนา หรือปรับปรุงระบบรักษาความปลอดภัยของข้อมูลและขั้นตอน การตรวจสอบสิทธิการใช้งานให้ทันสมัย										
5. การขาดกระบวนการภายในเพื่อจัดการ, สร้าง และควบคุมภายในองค์การ หมายถึง การที่องค์กรขาดระบบในการจัดการข้อมูล ทำให้การควบคุมการใช้ข้อมูลเป็นไปอย่างลำบาก										
6. การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (Application) ระบบ (System) หรือ ซอฟต์แวร์ (Software) ที่มีการแก้ไขเปลี่ยนแปลง หมายถึง เมื่อมีการแก้ไขหรือเปลี่ยนแปลงข้อมูลบนระบบ แล้วไม่มีการทำบันทึกหรือแจ้งผู้เกี่ยวข้องทราบ ดังนั้นเมื่อเกิดปัญหาขึ้นจะไม่สามารถตรวจสอบย้อนกลับได้ว่าเกิดจากสาเหตุใด										
7. มีการแก้ไขโปรแกรมประยุกต์ (Application) อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (Code) โดยไม่มีการทดสอบ										
8. กระบวนการควบคุมต่างๆ มีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่มีความใส่ใจ ทำให้เกิดการใช้งานที่ผิดพลาด เนื่องจากไม่เข้าใจขั้นตอนในการเข้าใช้งาน										

คำถามด้าน Availability - การเข้าถึงข้อมูลต่าง ๆ ได้เมื่อต้องการ	โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ					ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ				
	1 ไม่เกิด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด	1 ต่ำสุด	2 ต่ำ	3 ปานกลาง	4 มาก	5 มากที่สุด
1. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์การได้ หมายถึง การบุกรุกโดยการเจาะระบบรักษาความปลอดภัยเข้ามาถึงเครื่อง Server ภายในองค์การได้ไม่ว่าเทคนิควิธีใดก็ตาม										
2. การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับจนเกินไป										
3. การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง										
4. ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย เช่น ผู้ชมภายนอกเข้าใช้งาน และดูข้อมูลใน Website ขององค์การจำนวนมากในเวลาเดียวกัน										
5. การดูแลรักษา (Maintenance) ระบบ ทำให้ระบบไม่สามารถใช้งานได้ หมายถึง การที่ผู้ดูแลระบบการตรวจสอบและปิดเครื่อง Server ในช่วงเวลาที่มีการใช้งานของผู้ใช้ จึงเกิดการขัดจังหวะในการทำงาน										
6. งบประมาณในการสำรอง (Backup) ข้อมูลไม่เพียงพอ หมายถึง การขาดงบประมาณสำหรับค่าใช้จ่ายของอุปกรณ์ และการติดตั้งการวางระบบสำรองข้อมูลขององค์การ										
7. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม หมายถึง การที่พนักงานขาดการสร้างความรู้ ความเข้าใจในการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์การไม่ได้รับอบรมความรู้ใหม่ เมื่อมีการเปลี่ยนแปลงรูปแบบการทำงาน หรือระบบที่ใช้งานจากแบบเดิม										
8. Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ หมายถึง การที่ระบบเกิดความไม่ปลอดภัย เนื่องจากอุปกรณ์เครือข่ายขัดข้องทำให้การเชื่อมต่อไปยังข้อมูลที่ต้องการถูกตัดขาด และเสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดี										
9. ข้อมูลที่เก็บสำรอง (Backup) ไม่เพียงพอ หมายถึง ไม่ได้มีการสำรองข้อมูลแบบทั้งหมด (Full Backup) ทำให้เกิดปัญหาเมื่อต้องการข้อมูลส่วน ที่ไม่ได้สำรองข้อมูลไว้										

ขอขอบพระคุณเป็นอย่างสูงที่ได้สละเวลาอันมีค่าในการออกแบบสอบถามโครงการวิจัยในครั้งนี้

ข้อมูลที่ได้จะนำมาวิเคราะห์ในภาพรวมและไม่เปิดเผยข้อมูลส่วนบุคคลใด ๆ ในแบบสอบถามนี้

วิภาวรรณ คุ้มศิริ

คำอธิบายเกณฑ์การให้คะแนน

หมวด : โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์การ

1 ไม่เกิด = ไม่มีโอกาสเกิดความเสี่ยงขึ้นเลย โอกาสเกิดเป็น 0 %

2 ต่ำ = มีโอกาสเกิดความเสี่ยงขึ้นประมาณ 1 - 25 %

3 ปานกลาง = มีโอกาสเกิดความเสี่ยงขึ้นประมาณ 25 - 50 %

4 มาก = มีโอกาสเกิดความเสี่ยงขึ้นประมาณ 51 - 75 %

5 สูงมาก = มีโอกาสเกิดความเสี่ยงขึ้นประมาณ 76 - 100 %

หมวด : ระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นในองค์การ

1 ต่ำสุด = ไม่มีผลกระทบต่อองค์การเลย ผลกระทบเป็น 0 %

2 ต่ำ = มีผลกระทบต่อองค์การประมาณ 1 - 25 %

3 ปานกลาง = มีผลกระทบต่อองค์การประมาณ 25 - 50 %

4 มาก = มีผลกระทบต่อองค์การประมาณ 51 - 75 %

5 สูงมาก = มีผลกระทบต่อองค์การประมาณ 76 - 100 %