ผนวก ข

ตัวอย่างแบบสอบถาม การสำรวจความปลอดภัยด้านสารสนเทศภายในองค์กรที่ให้บริการด้านการจัดซื้อออนไลน์ (e-Procurement)

แบบสอบถาม

การสำรวจความปลอดภัยด้านสารสนเทศภายในองค์กรที่ให้บริการด้านการจัดซื้อออนไลน์(e-Procurement)

หากพบข้อสงสัยในแบบสอบถาม กรุณาติดต่อ

นางสาวเพ็ญประภา พิพัฒนาโฆษิต เบอร์โทรศัพท์: 081-937-0078 อีเมล์: tiorny@gmail.com

วัตถุประสงค์

เพื่อศึกษาแนวทางสำหรับการประยุกต์ใช้ มาตรฐานสากล ISO 17799 ในการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร ที่ให้บริการด้านการจัดซื้อออนไลน์(e-Procurement) และเพื่อจัดทำข้อสรุปในส่วนที่องค์กรควรพัฒนาและปรับปรุง

(โดยใช้เพื่องานวิจัยเฉพาะกรณีของนักศึกษาหลักสูตรบริหารเทคโนโลยี วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์)

คำชี้แจง

แบบสอบถาม แบ่งออกเป็น 3 ส่วน ได้แก่

ส่วนที่ 1 คำถามข้อมูลทั่วไป

ส่วนที่ 2 คำถามข้อมูลในการแสดงความคิดเห็น ด้านการรักษาความปลอดภัยของระบบสารสนเทศ (โดยในที่นี้ระบบสารสนเทศประกอบไปด้วย ข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่ายต่างๆในองค์กร)

ส่วนที่ 3 คำถามข้อมูลในการแสดงความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษาความปลอดภัยในองค์กร **(คำถามเฉพาะพนักงานที่มีหน้าที่ดูแลทางด้าน ระบบสารสนเทศ -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 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 ระยะเวลาการทำงานที่องค์กรปัจจุบัน

☐ < 1 ปี ☐ 1-2 ปี ☐ 3-4 ปี ☐ > 4 ปี

1.6 ตำแหน่งงานในองค์กร

☐ ระดับปฏิบัติการ ☐ ระดับบริหาร

1.7 หน่วยงานที่สังกัดในองค์กร

☐ หน่วยงานทางด้าน IT เช่น Software development , Helpdesk , Technical Operation เป็นต้น

☐ หน่วยงานทางด้านการให้คำปรึกษา หรือการให้ข้อมูลต่างๆ เช่น Sourcing , Consulting เป็นต้น

☐ หน่วยงานทางด้านการขาย หรือ วางแผนการตลาด เช่น Marketing , Sale

☐ หน่วยงานด้านการเงิน การบัญชี และหน่วยงานที่ต้องประจำตามต่างจังหวัด

☐ หน่วยงานทางด้านการประชาสัมพันธ์ม ฝ่ายโฆษณา , ฝ่ายธุรการ และอื่นๆ .....

ส่วนที่ 2 ข้อมูลในการแสดงความคิดเห็น ด้านการรักษาความปลอดภัยระบบสารสนเทศในองค์กร

1	คำถามด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
1.1	ท่านทราบหรือไม่ว่าปัจจุบันองค์กรมีการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร(กรณีที่ไม่ทราบ ข้ามไปทำข้อ 2) (1= ไม่ทราบ , 5 = ทราบ)					
1.2	ท่านทราบรายละเอียดของนโยบายดังกล่าวหรือไม่ (1= ไม่ทราบ , 5 = ทราบ)					
1.3	ท่านทราบแหล่งที่สามารถเข้าไปอ่านนโยบายดังกล่าวหรือไม่ (1= ไม่ทราบ , 5 = ทราบ)					

2	คำถามด้าน โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
2.1	ท่านทราบหน้าที่ความผิดชอบของท่านในการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยเพียงใด					
2.2	ท่านทราบเรื่องการรักษาและไม่เปิดเผยความลับขององค์กรมากน้อยเพียงใด					
2.3	ท่านเห็นว่ามาตรฐานขององค์กรในการให้บริการธุรกรรมออนไลน์ ปัจจุบันมีความปลอดภัยด้านข้อมูลมากน้อยเพียงใด					

3	คำถามด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
3.1	ท่านทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศมากน้อยแค่ไหน					
3.2	ท่านสามารถแบ่งประเภทของข้อมูลได้มากน้อยแค่ไหน เช่น ข้อมูลลับ(Secret Information),ข้อมูลลับเฉพาะ(Confidential Information),ข้อมูลที่จำเป็นมาก(Critical Information),ข้อมูลสาธารณะหรือข้อมูลทั่วไป					

4	คำถามด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
4.1	ท่านคิดว่าการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ต่างๆภายในองค์กรมีความเหมาะสมเพียงใดในปัจจุบัน					
4.2	ท่านเคยได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยแค่ไหน					
4.3	ท่านทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรมากน้อยแค่ไหน					

5	คำถามด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
5.1	ท่านคิดว่าปัจจุบันบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่สำคัญ มีความเหมาะสมหรือความปลอดภัยมากน้อยเพียงใด					

5	**คำถามด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)**	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
5.2	ท่านคิดว่าการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัย มีความเหมาะสมหรือปลอดภัยมากน้อยเพียงใด					
5.3	ท่านมีการระวังและป้องกันอุปกรณ์จากอุบัติเหตุต่างๆมากน้อยเพียงใด เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชน หรือ เสี่ยงต่อการเกิดเข้าใช้งานจากผู้ไม่มีสิทธิ เป็นต้น					
5.4	ท่านคิดว่าองค์กรมีการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานมากน้อยเพียงใด					

6	**คำถามด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)**	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
6.1	หน่วยงานของท่านมีการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรสม่ำเสมอมากน้อยเพียงใด					
6.2	ท่านเห็นว่าองค์กรมีการบริหารจัดการเครือข่าย (Network controls)และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์(Application)ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายมีเหมาะสมมากน้อยเพียงใด					
6.3	ท่านให้ความสำคัญในการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้องมากน้อยเพียงใด					
6.4	ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร มากน้อยเพียงใด					
6.5	ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรมากน้อยเพียงใด					
6.6	ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมลล์ขององค์กรมากน้อยเพียงใด					
6.7	ท่านเห็นว่าองค์กรมีการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT สม่ำเสมอมากน้อยเพียงใด					

7	**คำถามด้าน การควบคุมการเข้าถึง (Access control)**	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
7.1	ท่านทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรมากน้อยเพียงใด					
7.2	ถ้าองค์กรมีการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ท่านทราบตามระยะที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน) ท่านเห็นด้วยมากน้อยเพียงใด					
7.3	ท่านให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อท่านไม่อยู่เป็นเวลานาน เช่น ประชุม, ทานอาหารกลางวัน มากน้อยเพียงใด					
7.4	ท่านให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ท่านใช้งานมากน้อยเพียงใด					
7.5	ท่านให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรมากน้อยเพียงใด					
7.6	ท่านเห็นว่ามาตรฐานการใส่ User ID & Password ก่อนเข้าใช้งานระบบต่างๆภายในองค์กร (ระบบบริหารจัดการรหัสผ่าน - Password management system) มีความเหมาะสมและปลอดภัยมากน้อยเพียงใด					

7	**คำถามด้าน การควบคุมการเข้าถึง** (Access control)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
7.7	ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กรมากน้อยเพียงใด เช่น โปรแกรม Photoshop , ACDSee หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์					
7.8	ท่านมีการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรมากน้อยเพียงใด ตัวอย่าง การScan ไวรัสใน Handy drive ก่อนใช้งาน ฯลฯ					

8	**คำถามด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ** (Information systems acquisition, development and maintenance)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
8.1	ท่านเคยประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลบ้างหรือไม่และมากน้อยเพียงใด (1 = ไม่เคย 0%, 2 = พบประมาณ 1%-25%, 3 = พบประมาณ 26%-50% , 4 = พบประมาณ 51%-75% , 5 = พบประมาณ 76%-100%)					
8.2	ท่านเคยประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนบ้างหรือไม่และมากน้อยเพียงใด (1 = ไม่เคย 0%, 2 = พบประมาณ 1%-25%, 3 = พบประมาณ 26%-50% , 4 = พบประมาณ 51%-75% , 5 = พบประมาณ 76%-100%)					
8.3	เมื่อท่านประสบปัญหาต่างๆดังกล่าวท่านได้ทำการแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดหรือไม่ กรณีผู้ที่ไม่เคยประสบปัญหาใดๆการใช้งานขอให้ข้ามไปข้อต่อไป (1 = ไม่เคยแจ้ง, 3 = แจ้ง แต่ไม่ทุกครั้ง , 5 = แจ้งทุกครั้งที่พบ)					

9	**การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร** (Information security incident management)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
9.1	ท่านคิดว่าซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรมีความเหมาะสมมากน้อยเพียงใด					
9.2	ท่านเคยรายงานเหตุการณ์หรือรายงานจุดอ่อน จุดบกพร่องที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่มากน้อยเพียงใด					

10	**การบริหารความต่อเนื่องในการดำเนินงานขององค์กร** (Business continuity management)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
10.1	ท่านเห็นว่าปัจจุบันการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีมากน้อยเพียงใด					

11	**การปฏิบัติตามข้อกำหนด** (Compliance)	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
11.1	ท่านเคยลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรหรือไม่ (1= ไม่เคย , 5 = เคย)					
11.2	ท่านเห็นว่าการเข้ารหัสข้อมูล เช่น การเข้าดูข้อมูล การผ่านเข้าออกในส่วนสำคัญต่างๆขององค์กร หรือการเข้าใช้งานอุปกรณ์ต่างๆมีความเข้มงวดและปลอดภัยมากน้อยเพียงใด					
11.3	ปัจจุบันผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของท่าน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร มากน้อยเพียงใด					

การระบุด้านความเสี่ยง ด้าน Confidentiality - สิทธิในการเข้าถึงเข้ามูลต่าง ๆ	1 (น้อยที่สุด)	2 (น้อย)	3 (ปานกลาง)	4 (มาก)	5 (มากที่สุด)
1 การรักษารหัสผ่าน (Password) ของส่วนบุคคลอย่างไม่เหมาะสม					
โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร (1 = ไม่เกิด , 2 = น้อย , 3= ปานกลาง ,4 = มาก , 5 = มากที่สุด)					
ระดับความรุนแรงของความเสี่ยง(Impact)หากเกิดความเสี่ยงขึ้นในองค์กร					
2 การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด					
โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร (1 = ไม่เกิด , 2= น้อย , 3 = ปานกลาง , 4 = มาก , 5 = มากที่สุด)					
ระดับความรุนแรงของความเสี่ยง(Impact)หากเกิดความเสี่ยงขึ้นในองค์กร					
3 การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล					
โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร (1 = ไม่เกิด , 2= น้อย , 3 = ปานกลาง , 4 = มาก , 5 = มากที่สุด)					
ระดับความรุนแรงของความเสี่ยง(Impact)หากเกิดความเสี่ยงขึ้นในองค์กร					

ท่านเคยพบปัญหาเรื่องการใช้งานระบบภายในองค์กรด้านใดบ้าง

ส่วนที่ 3 ข้อมูลการแสดงความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยในองค์กร(เฉพาะพนักงานที่มีหน้าที่ดูแลทางด้าน ระบบสารสนเทศ -IT)

ความเสี่ยง ด้าน Confidentiality - สิทธิในการเข้าถึงเข้ามูลต่าง ๆ		โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร					ระดับความรุนแรงของความเสี่ยง (Impact)หากเกิดความเสี่ยงขึ้นใน				
		0	1	2	3	4	0	1	2	3	4
		ไม่เกิด	ต่ำ	ปานกลาง	สูง	สูงมาก	ต่ำสุด	ต่ำ	ปานกลาง	สูง	สูงมาก
1	การเข้าถึงข้อมูลจากผู้ที่ไม่สิทธิใช้งานจริง *										
2	การระบุชื่อข้อมูลที่สร้างขึ้นไม่ถูกต้อง										
3	การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง										
4	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม *										
5	การเข้าใช้ข้อมูลสำรอง (Back up) โดยปราศจากการควบคุม *										

ความเสี่ยง ด้าน Integrity - ความถูกต้องสมบูรณ์ของข้อมูล		โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร					ระดับความรุนแรงของความเสี่ยง (Impact)หากเกิดความเสี่ยงขึ้นใน				
		0	1	2	3	4	0	1	2	3	4
		ไม่เกิด	ต่ำ	ปานกลาง	สูง	สูงมาก	ต่ำสุด	ต่ำ	ปานกลาง	สูง	สูงมาก
1	การเกิดความผิดพลาดในการรายงานผลข้อมูล										
2	ข้อมูลภายในองค์กรขาดการพัฒนาหรืออัพเดท(Update)ให้ทันสมัย										
3	ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน(corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด *										
4	การขาดการพัฒนา หรือปรับปรุง ระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานให้ทันสมัย										
5	การขาดกระบวนการภายในเพื่อจัดการ,สร้าง,และควบคุมข้อมูลภายในองค์กร *										
6	การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์(application) ระบบ(system) หรือ ซอฟแวร์(Software)ที่มีการแก้ไขเปลี่ยนแปลง										
7	มีการแก้ไขโปรแกรมประยุกต์(Application)อย่างไม่ถูกต้อง เช่น แก้ไขรหัส(code) โดยไม่มีการทดสอบ *										
8	กระบวนการควบคุมต่างๆมีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่ให้ความใส่ใจ *										

ความเสี่ยง ด้าน Availability - การเข้าถึงข้อมูลต่าง ๆได้เมื่อต้องการ		โอกาสในการเกิดความเสี่ยง (Likelihood)ภายในองค์กร					ระดับความรุนแรงของความเสี่ยง (Impact)หากเกิดความเสี่ยงขึ้นใน				
		0	1	2	3	4	0	1	2	3	4
		ไม่เกิด	ต่ำ	ปานกลาง	สูง	สูงมาก	ต่ำสุด	ต่ำ	ปานกลาง	สูง	สูงมาก
1	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ *										
2	การออกแบบระบบซับซ้อนเกินไป *										
3	การติดตั้งฮาร์ดแวร์หรือซอฟแวร์ไม่ถูกต้อง *										
4	ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย										
5	การดูแลรักษา(maintenance)ระบบ ทำให้ระบบไม่สามารถใช้งานได้ *										
6	งบประมาณในการสำรอง (Back up) ข้อมูลไม่เพียงพอ *										
7	พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม *										
8	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ *										
9	ข้อมูลที่เก็บสำรอง (Back up)ไม่เพียงพอ *										
10	การสูญเสียลูกค้าเนื่องจากระบบภายในขององค์กรไม่สามารถให้บริการได้										

ขอขอบพระคุณเป็นอย่างสูงที่ได้สละเวลาอันมีค่าในการกรอกแบบสอบถามโครงการวิจัยในครั้งนี้

ข้อมูลที่ได้จะนำมาวิเคราะห์ในภาพรวมและไม่เปิดเผยข้อมูลส่วนบุคคลใดๆในแบบสอบถามนี้

เพ็ญประภา พิพัฒนาโฆษิต

หมายเหตุ : * เป็นคำถามจากแบบสอบถามเดิมของผลงานวิจัยเรื่อง "การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูล สำหรับองค์กรขนาดกลางและขนาดใหญ่ในเขตกรุงเทพมหานคร." โดย คุณทรงชล มหารมณ์