ภาคผนวก

ภาคผนวก ก

Information Risk Management for Data Security Systems Requirements (LSD_D001)

Information Risk Management for Data Security Systems Requirements
อ้างอิงจาก: มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ ISO/IEC 27001: 2005Documents No. : LSD_D001

1. นโยบายความมั่นคงปลอดภัย (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรเพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document) (ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษรเอกสาร นโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy) (ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization) มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security) (ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัยโดยมีการกำหนดทิศทางที่ชัดเจนการกำหนดคำมั่นสัญญาที่ชัดเจน และการปฏิบัติที่สอดคล้องการมอบหมายงานที่

เหมาะสมต่อบุคลากร พร้อมทั้งการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Informationsecurity coordination) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities) (ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities) (ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality Agreements) (หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

2.1.6 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties) มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัย สำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึงถูกประมวลผลหรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศ โดยหน่วยงานภายนอก (Identification of risks related to external parties) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอกและกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers (หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรเมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กรก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements) (หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอกเมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กรก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas) มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตการก่อให้เกิดความเสียหายและการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

1. การจัดทำบริเวณล้อมรอบ (Physical security perimeter)(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่กั้นบริเวณจัดทำผนังหรือกำแพงล้อมรอบจัดทำประตูทางเข้า-ออกที่มีการควบคุมตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงานเป็นต้นเพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

2. การควบคุมการเข้า-ออก (Physical entry controls) (หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

3. การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting againstexternal and environmental threats) (หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆได้แก่ไฟไหม้น้ำท่วมแผ่นดินไหวการระเบิดความไม่สงบของบ้านเมืองหรือหายนะอื่นๆทั้งที่เกิดจากมนุษย์และธรรมชาติ

4. การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working insecure areas) (หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

5. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas) (หัวหน้างานอาคารและหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาตและถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมาต่างหาก

ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

มีจุดประสงค์เพื่อป้องกันการสูญหายการเกิดความเสียหายการถูกขโมยหรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กรและการทำให้กิจกรรมการดำเนินงานต่างๆขององค์กรเกิดการติดขัดหรือหยุดชะงัก

1. การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection) (พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆรวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ระบบกระแสไฟฟ้าระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง และระบบสายสื่อสารสำรอง เป็นต้น

3. การเดินสายไฟสายสื่อสารและสายเคเบิ้ลอื่นๆ (Cabling security) (หัวหน้างานอาคารและหัวหน้างานสารสนเทศ) ต้องกำหนดให้การเดินสายไฟฟ้าสายสื่อสารและสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึง โดยไม่ได้รับอนุญาตการทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

4. การบำรุงรักษาอุปกรณ์ (Equipment maintenance) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆอย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

5. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Securedisposal or re-use of equipment) (พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าว ได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

6. การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property) (หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กรได้แก่อุปกรณ์สารสนเทศหรือซอฟต์แวร์ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations management)

การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Operational Procedures and Responsibilities)

1. มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures) (หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงานปรับปรุงตามระยะเวลาอันสมควรและแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

1.2 การควบคุมการเปลี่ยนแปลงปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลงปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties) (ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

2. การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party Service Delivery Management) มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัยลักษณะของการให้บริการและระดับของการให้บริการ

2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring andreview of third party services) (หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่นการดูจากการให้บริการการศึกษาจากรายงาน และข้อมูลต่างๆที่กำหนดให้บันทึกไว้เป็นต้น

2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changesto third party services) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบ หรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่นการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับ การรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

3. การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance) มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management) (หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

3.2 การตรวจรับระบบ (System acceptance) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติมหรือที่เป็นรุ่นใหม่รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

4. การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code) มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code) (ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับการป้องกันและการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีรวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code) (ผู้ดูแลระบบ) ต้องมีมาตรการ เพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่ง เพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

5. การสำรองข้อมูล (Back-up) มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.1 การสำรองข้อมูล (Information back-up) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6. การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network Security Management) มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือค่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

6.1 มาตรการทางเครือข่าย (Network controls) (ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่ายกำหนดมาตรการ เพื่อป้องกันภัยคุกคามต่างๆทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชัน ที่ใช้งานเครือข่ายรวมทั้งสารสนเทศต่างๆที่ส่งผ่านทางเครือข่าย

6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of networkservices) (หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการ สำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้ อาจจะเป็นบริการเครือข่ายภายในขององค์กรเอง หรือบริการที่ได้รับจากหน่วยงานภายนอก

7. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling) มีจุดประสงค์เพื่อป้องกันการเปิดเผยการเปลี่ยนแปลง แก้ไขการลบหรือการทำลายทรัพย์สินสารสนเทศ โดยไม่ได้รับอนุญาตและการติดขัดหรือหยุดชะงักทางธุรกิจ

7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Managementof removable media) (หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media) (หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้วการทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handlingprocedures) (หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

8. การแลกเปลี่ยนสารสนเทศ (Exchange of Information) มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศ และซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures) (ผู้บริหารองค์กร) ต้องกำหนดนโยบายขั้นตอนปฏิบัติและมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements) (หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร

8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit) (หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึง โดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

9. การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services) มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

9.2 การทำธุรกรรมออนไลน์ (On-line transactions) (หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศ ที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

10. การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring) มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Auditlogging) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้การปฏิเสธการให้บริการของระบบและเหตุการณ์ต่างๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมออาทิเพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆที่เกี่ยวข้องกับการใช้งานสารสนเทศเพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ(Administrator and operator logs) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

10.5การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization) (ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

การควบคุมการเข้าถึง (Access control)

ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access control) มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ

1. นโยบายการควบคุมการเข้าถึงระบบ (Access control policy) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้การจัดทำนโยบายนี้ จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

2. การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management) มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.1 การลงทะเบียนพนักงาน (User registration) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งานเช่นเมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กรเป็นต้น

2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management) (ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) (ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการเพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) (หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

3.1 การใช้งานรหัสผ่าน (Password use) (ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

3.2 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy) (ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สิน

สารสนเทศที่สำคัญเช่นเอกสารสื่อบันทึกข้อมูลอยู่ในสถานที่ที่ไม่ปลอดภัยเช่นสามารถเข้าถึงได้ทางกายภาพอยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่ายเป็นต้น

4. การควบคุมการเข้าถึงเครือข่าย (Network Access control) มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) (ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่า บริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้บริการใดไม่สามารถใช้งานได้

4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) (ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กร สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification innetworks) (ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุ และพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remotediagnostic and configuration port protection) (ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบมาตรการต้องครอบคลุม ทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

4.5 การแบ่งแยกเครือข่าย (Segregation in networks) (ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งานกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ

4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) (ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรการเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางธุรกิจได้ระบุ

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system Access control) มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-onprocedures) (ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification andauthentication) (ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกันและต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system) (ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

5.4การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out) (ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

5.5การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connectiontime) (ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

6. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access control) มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอปพลิเคชันโดยไม่ได้รับอนุญาต

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)(ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) (หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

7. มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing andcommunications) (ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) (ผู้บริหารสนเทศ) ต้องกำหนดนโยบายแผนงานและขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

1. ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems) มีจุดประสงค์เพื่อให้การจัดหา และการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification) (ผู้พัฒนาและผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

2. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management) มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

2.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆที่ใช้งานประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

1. การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses) มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events) (พนักงานหรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรโดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses) (พนักงานหรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงานหรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

2. การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incident sand Improvements) มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures) (หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรและขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผลและมีความเป็นระบบระเบียบที่ดี

2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents) (ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัยโดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence) (หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎ หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

1. หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information Security Aspects of Business Continuity Management) มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศและเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including informationsecurity in the business continuity management process) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจการบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอกระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Businesscontinuity and risk assessment) (หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงักโอกาสที่จะเกิดขึ้นผลกระทบที่เป็นไปได้รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security) (ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัดหยุดชะงักหรือล้มเหลว

1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework) (ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจเพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกันครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้และจัดลำดับความสำคัญของงานต่างๆที่ต้องดำเนินการ

1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing maintaining and re-assessing business continuity plans) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอเพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

การปฏิบัติตามข้อกำหนด (Compliance)

1. การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements) มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมายระเบียบปฏิบัติข้อกำหนดในสัญญาและข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

1.1 การระบุข้อกำหนดต่างๆที่มีผลทางกฎหมาย (Identification of applicable legislation) (หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมายทางด้านระเบียบปฏิบัติและที่ปรากฏในสัญญา (ระหว่างองค์กรและบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กรต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษรและปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอรวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

1.2 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection oforganizational records) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติข้อกำหนดที่ปรากฏในสัญญาและข้อกำหนดทางธุรกิจจากการสูญหายการถูกทำลายให้เสียหายและการปลอมแปลง

1.3 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities) (หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

2. การปฏิบัติตามนโยบายมาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with Security Policies and Standards, and Technical Compliance) มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

2.1 การปฏิบัติตามนโยบายและมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards) (ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับดูแลและควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ ความรับผิดชอบของตนทั้งนี้ เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technicalcompliance checking) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอเพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

3. การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations) มีจุดประสงค์ เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systemsaudit controls) (หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบ

สารสนเทศขององค์กรเพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจเช่นการหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน

3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools) (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่นซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

ภาคผนวก ข

Internal Audit Manual (LSD_D002)

ตัวอย่างเอกสาร Internal Audit Manual (LSD_D002) ซึ่งเป็นแนวทางปฏิบัติและตรวจสอบด้านความปลอดภัยของข้อมูลในระบบบริหารจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล บริษัท ลำพูนซิงเด็นเก็น จำกัด

LSD **Internal Audit Manual**

Audit Manual For Information Risk Management for Data Security

Doc. No. : LSD_D002
Edit : 1
Page ___of___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005

Checklist	Standard (Reference)	Section	Detail
1. นโยบายความมั่นคงปลอดภัย (Security policy)			
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ Information security policy	จุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	> องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร และควรได้รับอนุมัติจากผู้บริหาร และเผยแพร่เพื่อให้พนักงานได้รับทราบ โดย นโยบายฯ ควรสอดคล้องหรือตรงกับความต้องการทางธุรกิจขององค์กรและ แสดงเจตจำนงค์มั่นคงปลอดภัย ของผู้บริหารเพื่อให้พนักงานเห็นถึงความสำคัญของการรักษาความและควรกล่าวถึงหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน
	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	> องค์กรควรกำหนดผู้มีหน้าที่รับผิดชอบในการตรวจสอบและปรับปรุงนโยบายเพื่อให้มีความทันสมัยอยู่เสมอ > องค์กรควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัยและควรกำหนดรอบระยะเวลาที่ชัดเจนในการตรวจสอบและปรับปรุงนโยบาย > องค์กรควรมีการประเมินผลและผลกระทบอันเกิดจากการเปลี่ยนแปลงทางเทคโนโลยีที่มีต่อนโยบายความมั่นคงปลอดภัย
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)			
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)	จุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
2.1.1	2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	> องค์กรควรมีการแต่งตั้งหรือกำหนดคณะทำงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และคณะทำงานฯ ควรมีบุคลากรที่เป็นตัวแทนจากทุกหน่วยงานภายในองค์กร > คณะทำงานฯ ควรมีบทบาทและหน้าที่ความรับผิดชอบที่ชัดเจนในการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ > คณะทำงานฯ ควรมีความเกี่ยวข้องกับการตรวจสอบ ปรับปรุง และอนุมัติการใช้งานนโยบายความมั่นคงปลอดภัย > คณะทำงานฯ ควรทำหน้าที่ในการกำหนดทรัพยากรที่จำเป็นสำหรับการบริหารจัดการความมั่นคงปลอดภัย > คณะทำงานฯ ควรมีหน้าที่ในการเฝ้าระวังภัยคุกคามหรือแนวโน้มของปัญหาด้านความมั่นคงปลอดภัยที่มีต่อองค์กร

2.1.2	2.1.2	การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	> คณะทำงานฯ ควรทำหน้าที่เป็นผู้ประสานงานสำหรับการดำเนินการต่างๆ ด้านความมั่นคงปลอดภัย > คณะทำงานฯ ควรทำหน้าที่ในการประเมินความเหมาะสมหรือความเพียงพอของมาตรการความมั่นคงปลอดภัยที่จะนำมาใช้กับระบบงานหรือบริการใหม่ขององค์กร > คณะทำงานฯ ควรมีส่วนร่วมหรือทำหน้าที่ในการตรวจสอบและประเมินเหตุการณ์ความมั่นคงปลอดภัยที่สำคัญๆ ที่เกิดขึ้น
2.1.3	2.1.3	การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	> องค์กรควรกำหนดให้พนักงานมีหน้าที่รับผิดชอบในการดูแลและป้องกันทรัพย์สินสารสนเทศที่คนใช้งานหรือถือครอง > องค์กรควรกำหนดบทบาท หน้าที่ และความรับผิดชอบสำหรับบุคลากรที่เกี่ยวข้องกับกระบวนการในการรักษาความมั่นคงปลอดภัย > องค์กรควรกำหนดบทบาท หน้าที่และความรับผิดชอบของพนักงานและผู้ที่เกี่ยวข้องโดยให้ครอบคลุมถึงระบบเทคโนโลยีสารสนเทศและบริการสารสนเทศต่างๆ > องค์กรควรกำหนดบทบาท หน้าที่ และความรับผิดชอบของพนักงานผู้ปฏิบัติงานที่มาจากหน่วยงานภายนอก และผู้ที่เกี่ยวข้องอื่นๆ ในการรักษาความมั่นคงปลอดภัยให้กับองค์กร
2.1.4	2.1.4	กระบวนการอนุมัติการใช้งานระบบเทคโนโลยีสารสนเทศ (Authorization process for information processing facilities)	> องค์กรควรมีกระบวนการอนุมัติและกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ > ผู้มีอำนาจ อนุมัติควรตรวจสอบว่าระบบเทคโนโลยีสารสนเทศใหม่นั้นเป็นไปตามหรือสอดคล้องกับนโยบายหรือข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กรหรือไม่ > ผู้มีอำนาจอนุมัติควรทำหน้าที่ตรวจสอบว่าฮาร์ดแวร์หรือซอฟต์แวร์ใหม่ที่ได้รับนั้นสามารถใช้งานและเข้ากันได้กับระบบงานปัจจุบันหรือไม่ > ผู้มีอำนาจอนุมัติควรดำเนินการตรวจสอบเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ส่วนตัวที่นำมาใช้งานกับธุรกิจขององค์กรก่อนที่จะอนุญาตให้ใช้งาน > องค์กรควรมีกระบวนการควบคุมการจัดซื้อจัดจ้างระบบเทคโนโลยีสารสนเทศโดยให้อยู่ในอำนาจของหน่วยงานสารสนเทศขององค์กร
2.1.5	2.1.5	ข้อตกลงการไม่เปิดเผยความลับ (Confidentiality agreements)	> องค์กรควรระบุชนิดหรือประเภทของข้อมูล เช่น ข้อมูลลับ เปิดเผยได้ ส่วนบุคคล เป็นต้น ที่จำเป็นต้องมีการป้องกันตามความเหมาะสม > องค์กรควรป้องกันข้อมูลสำคัญหรือข้อมูลลับโดยจัดทำข้อตกลงการไม่เปิดเผยความลับระหว่างองค์กรกับผู้ที่ได้รับการว่าจ้างหรือผู้ที่จำเป็นต้องเข้าถึงข้อมูล > องค์กรควรจัดทำข้อตกลงการไม่เปิดเผยความลับโดยให้ครอบคลุมถึงประเด็นดังนี้ *(นิยามของข้อมูลสำคัญหรือข้อมูลลับ, ช่วงระยะเวลาของข้อตกลงการไม่เปิดเผยความลับ, หน้าที่ความรับผิดชอบที่ต้องปฏิบัติกับข้อมูลสำคัญหรือข้อมูลลับ, ผู้เป็นเจ้าของข้อมูลสำคัญหรือข้อมูลลับ, เงื่อนไขการใช้ข้อมูลสำคัญหรือข้อมูลลับ, การสงวนสิทธิ์ในการตรวจสอบกิจกรรมที่เกี่ยวข้องกับข้อมูลสำคัญหรือข้อมูลลับ, วิธีดำเนินการทางกฎหมายหากมีการละเมิดข้อตกลง)*
2.1.6	2.1.8	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Independent review of information security)	> องค์กรควรดำเนินการทบทวนกระบวนการบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ เช่น ปีละ 1 ครั้ง เป็นต้น > องค์กรควรดำเนินการทบทวนประเด็นดังต่อไปนี้ *(วัตถุประสงค์ด้านความมั่นคงปลอดภัย, มาตรการความมั่นคงปลอดภัย, นโยบายความมั่นคงปลอดภัย, กระบวนการด้านความมั่นคง เช่น กระบวนการสร้างความต่อเนื่องให้กับธุรกิจ เป็นต้น, ขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย)*

2.2	2.2	โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)	จุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและ อุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก
2.2.1	2.2.1	การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)	> องค์กรควรดำเนินการประเมินความเสี่ยงสำหรับกรณีที่จะมีการอนุญาตให้หน่วยงานภายนอกเข้าถึงระยะ ไกล หรือทรัพย์สินสารสนเทศอื่นๆ ขององค์กร > องค์กรควรกำหนดมาตรการควบคุมการเข้าถึงที่เหมาะสมกับระดับความสำคัญของทรัพย์สินสารสนเทศที่อนุญาตให้หน่วยงานภายนอกเข้าถึง
2.2.2	2.2.2	การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)	> องค์กรควรจัดทำข้อกำหนดหรือเงื่อนไขด้านความมั่นคงปลอดภัยดังนี้ก่อนที่จะอนุญาตให้ลูกค้าเข้าถึงระบบงานหรือสารสนเทศขององค์กร
2.2.3	2.2.3	การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)	> องค์กรควรจัดทำข้อกำหนดด้านความมั่นคงปลอดภัยซึ่งควรครอบคลุมประเด็นความเสี่ยงต่างๆ เมื่อจำเป็นต้องให้หน่วยงาน หรือบุคคลภายนอกเข้าถึง สารสนเทศ
3. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)			
3.1	5.1	บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)	จุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร
3.1.1	5.1.1	การจัดทำบริเวณล้อมรอบ (Physical security perimeter)	> องค์กรควรจัดให้มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง > องค์กรควรกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยทางกายภาพและจัดสภาพแวดล้อมให้สอดคล้องกับข้อกำหนดดังกล่าว > ประตูหรือทางเข้าพื้นที่ ที่มีระบบเทคโนโลยีสารสนเทศควรออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ > ประตูหรือทางเข้าสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรมีระบบที่สามารถล็อคได้เพื่อป้องกันการบุกรุกทางกายภาพ > สำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น > องค์กรควรแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศขององค์กรออกจากพื้นที่ที่มีการดูแลหรือบริหารจัดการโดยผู้ให้บริการภายนอก
3.1.2	5.1.2	การควบคุมการเข้า-ออก (Physical entry controls)	> องค์กรควรมีมาตรการเพื่อควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่ที่นั่น > องค์กรควรมีมาตรการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออก > องค์กรควรมีการจัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญเพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น > องค์กรควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของผู้ให้บริการภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ > องค์กรควรจัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ
3.1.3	5.1.4	การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)	> องค์กร ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ
3.1.4	5.1.5	การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	> องค์กรควรมีมาตรการควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ > องค์กรควรมีมาตรการห้ามการใช้อุปกรณ์ถ่ายภาพ วิดีโอ และเครื่องอัดเสียง ภายในพื้นที่หรือบริเวณที่มีความสำคัญ

ภาคผนวก ค

Risk Estimation (LSD_D003)

ตารางเมตริกซ์การประมาณความเสี่ยง (Risk Estimation) คือเอกสารกฎเกณฑ์ในการประมาณความเสี่ยงที่ตรวจพบ

Doc. No. : LSD_D003
Edit : 1

Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง)

ความรุนแรงและ ผลกระทบของความเสี่ยง (Impact)	โอกาสที่ความเสี่ยงจะเกิดขึ้น (Likelihood)				
	น้อยมาก (1),(VL)	น้อย (2), (V)	ปานกลาง (3), (M)	บ่อย (4), (H)	บ่อยมาก (5), (VH)
รุนแรงมาก (20) = VH					
รุนแรง (15) = V					
ปานกลาง (10) = M					
น้อย (5) = V					
น้อยมาก (1) = VL					

Risk Assessment Matrix

VH = มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก)	20	40	60	80	100
H = มีความเสี่ยงและผลกระทบ (เสี่ยง)	15	30	45	60	75
M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง)	10	20	30	40	50
L = มีความเสี่ยงและผลกระทบต่ำ (ต่ำ)	5	10	15	20	25
VL = มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก)	1	2	3	4	5

ภาคผนวก ต

Information Risk Management For Data Security Requirement & Audit Scope Matrix (LSD_F001)

ตัวอย่างการนำแบบฟอร์ม InformationRisk Management For Data Security Requirement & Audit Scope Matrix (LSD_F003) ใช้ในการศึกษาครั้งนี้

INFORMATION RISK MANAGEMENT FOR DATA SECURITY

REQUIREMENT & AUDIT SCOPE MATRIX

Form. No. : LSD_F001
Edit : 1 Eff.date :

Requirement	1. นโยบายความมั่นคงปลอดภัย (Security policy)	2. ระบบแลกสารร่วมกลาง (File Sharing : LSD DATA SERVER, LSD PS SERVER)	3. Database Server จำนวน 4 Server (ERP. System, MRP. System, HRMS, DB Systems)	4. Active Directory Database	5. ระบบฐานข้อมูลสำนักงาน (Service Support Systems : Mail Server, Web Server)	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
1. นโยบายความมั่นคงปลอดภัย (Security policy)								
1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)	●							
1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	●							
1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	●							
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)								
2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)								
2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการ ทางด้านความมั่นคงปลอดภัย (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 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบ อิสระ (Independent review of information security)	●							

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)	●							
3. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)								
3.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)								
3.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)						●	●	
3.1.2 การควบคุมการเข้า-ออก (Physical entry controls)						●	●	
3.1.3 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)						●	●	
3.1.4 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)						⊕	⊕	
3.1.5 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)						⊕	⊕	
3.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)						●	●	
3.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)						●	●	
3.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)						●	●	
3.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)						●	●	
3.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)						●	●	
3.2.5 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)						●		
3.2.6 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)						●	⊕	
4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations management)								
4.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Operational Procedures and Responsibilities)								
4.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)		●	●	●	●	●	●	
4.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ ประมวลผลสารสนเทศ (Change management)		●	●	●	●	●	●	
4.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)		●	●	●	●	●	●	
4.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party Service Delivery Management)								
4.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)		●	●	●	●	●	●	
4.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)		⊕	●	⊕	●	⊕	⊕	
4.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)		⊕	●	⊕	●	⊕	⊕	
4.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)								
4.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)						●	●	
4.3.2 การตรวจรับระบบ (System acceptance)			●			⊕	⊕	
4.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code								
4.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	●	●	●	●	●			
4.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)	⊕	⊕	⊕	⊕	⊕		●	

4.5 การสำรองข้อมูล (Back-up)								
4.5.1 การสำรองข้อมูล (Information back-up)	●	●	●	●	●			
4.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network Security Management)								
4.6.1 มาตรการทางเครือข่าย (Network controls)		●	●	●	●		●	
4.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)							●	
4.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)								
4.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)	●							
4.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	●							
4.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)	●	●	●	●	●			
4.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)	●	●	●	●	●			
4.8 การแลกเปลี่ยนสารสนเทศ (Exchange of Information)								
4.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)	●							
4.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)	⊕							
4.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)	⊕							
4.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)	●				●			
4.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)	⊕							
4.9.1 การทำธุรกรรมออนไลน์ (On-line transactions)	●							
4.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring								
4.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)		●	●	●	●		⊕	
4.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)	●							
4.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)	●	●	●	●	●			
4.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)	●	●	●	●	●			
4.10.5 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)	●	●	●	●	●			
5. การควบคุมการเข้าถึง (Access control)								
5.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access control)								
5.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	●							
5.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)								
5.2.1 การลงทะเบียนพนักงาน (User registration)		●	●	●	●			
5.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)		●	●	●	●			
5.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)		⊕	⊕	●	⊕			
5.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)		●	⊕	●	⊕			
5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)								
5.3.1 การใช้งานรหัสผ่าน (Password use)		⊕	⊕	●	⊕			
5.3.2 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)	●							
5.4 การควบคุมการเข้าถึงเครือข่าย (Network Access control)								
5.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	●							
5.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)		⊕	⊕	●	⊕			
5.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)							●	
5.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)							●	
5.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)							●	
5.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)							●	

5.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system Access control)								
5.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)		⊕	⊕	●	⊕			
5.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)		⊕	⊕	●	⊕			
5.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)		⊕	⊕	●	⊕			
5.5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out		⊕	⊕	●	⊕			
5.5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)		⊕	⊕	●	⊕			
5.6 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access control)								
5.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)		⊕	⊕	●	⊕			
5.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)		⊕	⊕	⊕	⊕	●		
5.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)								
5.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	●							
5.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	●							
6. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)								
6.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)								
6.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification		⊕	⊕	⊕	⊕			
6.2 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)								
6.2.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)		⊕	⊕	⊕	⊕		●	
7. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)								
7.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses)								
7.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events	●							
7.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	●							
7.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents and Improvements)								
7.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)	●	⊕	⊕	⊕	⊕	⊕	⊕	
7.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)	●	⊕	⊕	⊕	⊕	⊕	⊕	
7.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)	●	⊕	⊕	⊕	⊕	⊕	⊕	
8. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)								
8.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information Security Aspects of Business Continuity Management)								
8.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)	●							
8.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	●							
8.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)	●							
8.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework	●							
8.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)	●							

9. การปฏิบัติตามข้อกำหนด (Compliance)								
9.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements)								
9.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)	●							
9.1.2 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)	●	⊕	⊕	⊕	⊕			
9.1.3 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)	●					●	●	
9.2 การปฏิบัติตามนโยบายมาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with Security Policies and Standards, and Technical Compliance)								
9.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)	●							
9.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)	●	⊕	⊕	⊕	⊕	⊕	⊕	
9.3 การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations)								
9.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)	●	⊕	⊕	⊕	⊕	⊕	⊕	
9.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)	●							

ภาคผนวก ฆ

Internal Audit Checklist (LSD_F002)

ตัวอย่างการนำแบบฟอร์ม Internal Audit Checklist (LSD_F002) ใช้วางแผนการตรวจและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลในการศึกษาครั้งนี้

rt

Internal Audit Checklist

LSD

☑ Audit Checklist For Information Risk Management for Data Security

Form. No. : LSD_F002
Edit : 1
Page ___of___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005

Checklist	Standard (Reference)	Section	Audit Question	Audit Scope	Findings (OK / NC)
1. นโยบายความมั่นคงปลอดภัย (Security policy)					
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ **Information security policy**			
1.1.1	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	องค์กรมีนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากผู้บริหารและ เผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้อง ได้รับทราบ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
1.1.2	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	องค์กรมีการ ทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)					
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)			
2.1.1	2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	ผู้บริหาร มีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง รวมถึงการมอบหมายงานที่เหมาะสมต่อบุคลากร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.2	2.1.2	การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	ผู้บริหาร มีการกำหนด ตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.3	2.1.3	การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	ผู้บริหาร มีการกำหนดหน้าที่ความรับผิดชอบของพนักงาน ใน การดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.4	2.1.4	กระบวนการอนุมัติการใช้งานระบบเทคโนโลยีสารสนเทศ (Authorization process for information processing facilities)	ผู้บริหาร มีการกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับใช้งานกระบวนการนั้นๆ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	

2.1.5	2.1.5	ข้อตกลงการไม่เปิดเผยความลับ (Confidentiality agreements)	หัวหน้างานบุคคล มีการจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น)	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.6	2.1.8	การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ (Independent review of information security)	องค์กรควรดำเนินการทบทวนประเด็นดังต่อไปนี้ (วัตถุประสงค์ด้านความมั่นคงปลอดภัย, มาตรการความมั่นคงปลอดภัย, นโยบายความมั่นคงปลอดภัย, กระบวนการด้านความมั่นคง เช่น กระบวนการสร้างความต่อเนื่องให้กับธุรกิจ เป็นต้น, ขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัย)	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.2	2.2	โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)			
2.2.1	2.2.1	การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)	หัวหน้างานสารสนเทศ มีการกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการ เข้าถึงสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวล ผลสารสนเทศ จากหน่วยงานภายนอก และกำหนดมาตรการรองรับ ให้เหมาะสมก่อนที่จะอนุญาตหรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.2.2	2.2.2	การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)	หัวหน้างานสารสนเทศ มีการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้บุคคลภายนอก เข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.2.3	2.2.3	การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)	หัวหน้างานสารสนเทศ มีการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้หน่วยงานภายนอก เข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
3. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)					
3.1	5.1	บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)			
3.1.1	5.1.1	การจัดทำบริเวณล้อมรอบ (Physical security perimeter)	มีการจัดการกับพื้นที่ เพื่อป้องกันการเข้า ถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.1.2	5.1.2	การควบคุมการเข้า-ออก (Physical entry controls)	มีจัดให้มีการควบคุม การเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่าน เข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.1.3	5.1.4	การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)	ฝ่ายอาคาร มีจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	

3.1.4	5.1.5	การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	ฝ่ายอาคาร ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงาน ในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.1.5	5.1.6	การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)	หัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับ การเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.2	5.2	ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)			
3.2.1	5.2.1	การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)	พนักงาน มีการจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.2.2	5.2.2	ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)	หัวหน้างานสารสนเทศ มีการกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรองระบบสายสื่อสารสำรอง เป็นต้น หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.2.3	5.2.3	การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)	หัวหน้างานสารสนเทศ มีการกำหนดให้การเดินสาย ไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเสียหาย หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.2.4	5.2.4	การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	หัวหน้างานสารสนเทศ มีการกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
3.2.5	5.2.6	การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)	พนักงาน มีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและ ซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)	
3.2.6	5.2.7	การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)	การควบคุมไม่ให้นำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น มีการควบคุมหรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and Operations management)					
4.1	6.1	การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน (Operational Procedures and Responsibilities)			

4.1.1	6.1.1	ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	หัวหน้างานสารสนเทศ มีการจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตาม ระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.1.2	6.1.2	การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบเทคโนโลยีสารสนเทศ (Change management)	หัวหน้างานสารสนเทศ มีการกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.1.3	6.1.3	การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)	มีการกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.2	6.2	การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party Service Delivery Management)			
4.2.1	6.2.1	การให้บริการโดยหน่วยงานภายนอก (Service delivery)	หัวหน้างานสารสนเทศ มีการกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการและระดับของการให้บริการ หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.2.2	6.2.2	การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)	หน่วยงานสารสนเทศ มีการตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	

4.2.3	6.2.3	การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)	ผู้บริหารสารสนเทศมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ หรือปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.3	6.3	การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)			
4.3.1	6.3.1	การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)	หัวหน้างานสารสนเทศ มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน หรือไม่	6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.3.2	6.3.2	การตรวจรับระบบ (System acceptance)	หัวหน้างานสารสนเทศ มีการจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่มีการปรับปรุง หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบ หรือไม่	3. Database Server จำนวน 4 Server 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.4	6.4	การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection Against Malicious and Mobile Code)			
4.4.1	6.4.1	การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	ผู้ดูแลระบบ มีมาตรการสำหรับการตรวจจับ การป้องกันและการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
4.4.2	6.4.2	การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)	มีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.5	6.5	การสำรองข้อมูล (Back-up)			
4.5.1	6.5.1	การสำรองข้อมูล (Information back-up)	หัวหน้างานสารสนเทศ มีการจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	

4.6	6.6	การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network Security Management)			
4.6.1	6.6.1	มาตรการทางเครือข่าย (Network controls)	ผู้ดูแลระบบ มีการบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.6.2	6.6.2	ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)	หัวหน้างานสารสนเทศ มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดขององค์กร หรือไม่	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
4.7	6.7	การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media Handling)			
4.7.1	6.7.1	การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)	มีการกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.7.2	6.7.2	การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	หน่วยงานสารสนเทศ มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายเป็นไปอย่างมั่นคงและปลอดภัย หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.7.3	6.7.3	ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)	หน่วยงานสารสนเทศ มีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและ การจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
4.7.4	6.7.4	การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)	หน่วยงานสารสนเทศ มีการกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
4.8	6.8	การแลกเปลี่ยนสารสนเทศ (Exchange of Information)			
4.8.1	6.8.1	นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ(Information exchange policies and procedures)	ผู้บริหารองค์กร มีการกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.8.2	6.8.2	ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)	หน่วยงานสารสนเทศ มีการจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและ ซอฟต์แวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	

4.8.3	6.8.3	การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)	หน่วยงานสารสนเทศ มีการป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.8.4	6.8.4	การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)	หน่วยงานสารสนเทศ มีการกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 5. ระบบข้อมูลสนับสนุน	
4.9	6.9	การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)			
4.9.1	6.9.2	การทำธุรกรรมอิเล็กทรอนิกส์ (On-line transactions)	หน่วยงานสารสนเทศ มีการกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่ง ที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.10	6.10	การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)			
4.10.1	6.10.1	การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)	หน่วยงานสารสนเทศ มีการกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	
4.10.2	6.10.2	การตรวจสอบการใช้งานระบบ (Monitoring system use)	หน่วยงานสารสนเทศ มีการกำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
4.10.3	6.10.3	การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)	หน่วยงานสารสนเทศ มีการกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
4.10.4	6.10.4	บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)	หัวหน้างานสารสนเทศ มีการกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	

4.10.5	6.10.6	การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)	ผู้ดูแลระบบ มีการตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
5. การควบคุมการเข้าถึง (Access control)					
5.1	7.1	ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access control)	มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ		
5.1.1	7.1.1	นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)	ผู้บริหารสารสนเทศ มีการกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
5.2	7.2	การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)			
5.2.1	7.2.1	การลงทะเบียนพนักงาน (User registration)	หน่วยงานสารสนเทศ มีการกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออก หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
5.2.2	7.2.2	การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)	ผู้ดูแลระบบ มีการจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
5.2.3	7.2.3	การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)	ผู้ดูแลระบบ มีการจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
5.2.4	7.2.4	การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	หัวหน้างานสารสนเทศ มีการจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้ หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	
5.3	7.3	หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)			
5.3.1	7.3.1	การใช้งานรหัสผ่าน (Password use)	ผู้ดูแลระบบ มีการกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน หรือไม่	2. ระบบเอกสารส่วนกลาง 3. Database Server จำนวน 4 Server 4. Active Directory Database 5. ระบบข้อมูลสนับสนุน	

5.3.2	7.3.3	นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)	ผู้บริหารสารสนเทศ มีการจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
5.4	7.4	การควบคุมการเข้าถึงเครือข่าย (Network Access control)			
5.4.1	7.4.1	นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)	ผู้บริหารสารสนเทศ มีการจัดทำนโยบายการใช้งานเครือข่าย ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
5.4.2	7.4.2	การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)	ผู้ดูแลระบบ มีการกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้ หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.4.3	7.4.3	การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)	ผู้ดูแลระบบ มีการกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว หรือไม่	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
5.4.4	7.4.4	การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)	ผู้ดูแลระบบ มีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและ ปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย หรือไม่	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
5.4.5	7.4.5	การแบ่งแยกเครือข่าย (Segregation in networks)	ผู้ดูแลระบบ มีการทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ หรือไม่	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
5.4.6	7.4.6	การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)	ผู้ดูแลระบบ มีการจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กรการเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางธุรกิจได้ระบุ หรือไม่	7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
5.5	7.5	การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)			
5.5.1	7.5.1	ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)	ผู้ดูแลระบบ มีการจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.5.2	7.5.2	การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)	ผู้ดูแลระบบ มีการจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.5.3	7.5.3	ระบบบริหารจัดการรหัสผ่าน (Password management system)	ผู้ดูแลระบบ มีการจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพหรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	

5.5.4	7.5.5	การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)	ผู้ดูแลระบบ มีการกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.5.5	7.5.6	การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)	ผู้ดูแลระบบ มีการจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.6	7.6	การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access control)			
5.6.1	7.6.1	การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)	ผู้ดูแลระบบ มีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* 4. Active Directory Database *5. ระบบข้อมูลสนับสนุน*	
5.6.2	7.6.2	การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)	หน่วยงานสารสนเทศ มีการแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)	
5.7	7.7	การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)			
5.7.1	7.7.1	การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)	ผู้บริหารสารสนเทศ มีการกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palmและ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
5.7.2	7.7.2	การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)	ผู้บริหารสารสนเทศ มีการกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานของค์กรจากภายนอกสำนักงาน หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
6. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)					
6.1	8.1	ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)			
6.1.1	8.1.1	การวิเคราะห์และการระบุข้อกำหนดด้านความมั่นคงปลอดภัย(Security requirements analysis and specification)	ผู้พัฒนาหรือเจ้าของระบบ มีการวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน*	
6.2	8.6	การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)			

6.2.1	8.6.1	มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)	หน่วยงานสารสนเทศ มีการกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้ง กำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว หรือไม่	*2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
7. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)					
7.1	9.1	การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events and Weaknesses)			
7.1.1	9.1.1	การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)	พนักงาน มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
7.1.2	9.1.2	การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	พนักงาน มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
7.2	9.2	การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of Information Security Incidents and Improvements)			
7.2.1	9.2.1	หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)	หัวหน้างานสารสนเทศ มีการกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร หรือไม่ และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบ	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* *6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)* *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	
7.2.2	9.2.2	การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)	ผู้ดูแลระบบ มีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* *6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)* *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	
7.2.3	9.2.3	การเก็บรวบรวมหลักฐาน (Collection of evidence)	หัวหน้างานสารสนเทศ มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* *6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)* *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	

8. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)					
8.1	10.1	หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information Security Aspects of Business Continuity Management)			
8.1.1	10.1.1	กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)	ผู้บริหารสารสนเทศ มีการกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอหรือไม่ และกระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
8.1.2	10.1.2	การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	หัวหน้างานสารสนเทศ มีการระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรหรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
8.1.3	10.1.3	การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)	ผู้บริหารสารสนเทศ มีการจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงักหรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
8.1.4	10.1.4	การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ(Business continuity planning framework)	ผู้บริหารสารสนเทศ มีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆที่ต้องดำเนินการ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
8.1.5	10.1.5	การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)	ผู้บริหารสารสนเทศ มีการกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
9. การปฏิบัติตามข้อกำหนด (Compliance)					
9.1	11.1	การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)			
9.1.1	11.1.1	การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)	หน่วยงานสารสนเทศ มีการระบุข้อกำหนดทางด้านกฎหมายทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น)ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
9.1.2	11.1.3	การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)	หน่วยงานสารสนเทศ มีการกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจจากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน*	

9.1.3	11.1.5	การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)	หน่วยงานสารสนเทศ มีการป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) 6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER) 7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)	
9.2	11.2	การปฏิบัติตามนโยบายมาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with Security Policies and Standards, and Technical Compliance)			
9.2.1	11.2.1	การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)	ผู้บริหารสารสนเทศ มีการกำหนดให้ผู้บังคับบัญชาดอยกำกับ ดูแล และ ควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
9.2.2	11.2.2		หน่วยงานสารสนเทศ มีการกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* *6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)* *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	
9.3	11.3	การตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations)			
9.3.1	11.3.1	มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)	หน่วยงานสารสนเทศ มีการระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy) *2. ระบบเอกสารส่วนกลาง* *3. Database Server จำนวน 4 Server* *4. Active Directory Database* *5. ระบบข้อมูลสนับสนุน* *6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)* *7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)*	
9.3.2	11.3.2	การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)	หน่วยงานสารสนเทศ มีการกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	

ภาคผนวก ง

Internal Audit Report (LSD_F003)

แบบฟอร์มInternal Audit Report(LSD_F003) ใช้รายงานความเสี่ยงที่ตรวจพบในการตรวจสอบภายในที่ใช้ในการศึกษาครั้งนี้

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1

Page ___ of ___

Audit Plan No.	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee

ผลจากการตรวจสอบ																	
No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)														CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง				
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH

Lumphun Shindengen Co.,Ltd.

ภาคผนวก จ

Risk Management Report For Data Security

ตัวอย่างการนำแบบฟอร์ม Risk Management Report For Data Securityมาใช้ในรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ซึ่งเป็นการแสดงถึงประเด็นความเสี่ยงที่ตรวจพบในการตรวจครั้งนี้

Risk Management Report For Data Security

Audit Report For IT Risk Assessment for Data Security

รายงานการบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Measure (มาตรการ)	Operations (การดำเนินการ)	Risk Status (สถานะ)		
					CAR.	Plan / Edit	Acceptable
1	ข้อกำหนด 2.1.5	ระเบียบบริษัทไม่ได้ระบุให้มีการ	เพิ่มเรื่อง ข้อตกลงการไม่เปิดเผยความลับ	ปรับปรุง ทบทวน ระเบียบบริษัท		√	
	ข้อตกลงการไม่เปิดเผยความลับ	ลงนาม ระหว่างบริษัทกับพนักงาน	ไปในการเซ็นสัญญาจ้างงาน	(Plan : 30/10/2555)			
2	ข้อกำหนด 2.1.6	มีการทบทวนปีละ 1 ครั้งแต่ทบทวน					√
	การทบทวนด้านความมั่นคง	เฉพาะหัวข้อที่ถูก J-Sox ตรวจเท่านั้น					
	ปลอดภัย ระบบสารสนเทศ						
3	ข้อกำหนด 3.1.4	ไม่มีเอกสารการควบคุมการปฏิบัติ					√
	การป้องกันจากภายนอกและ	งานของบุคคลภายนอก					
	สิ่งแวดล้อม						
4	ข้อกำหนด 3.2.3	ไม่มีแผนผังการเชื่อมต่อระบบ	จัดทำแผนผังทาง Network, ไฟฟ้า	CAR NO : R2012-01	√		
	การเดินสายไฟ,สายสื่อสาร	Server (ไฟฟ้า, Network)					
5	ข้อกำหนด 3.2.4	ปี 2011 ไม่ได้ปฏิบัติตามแผน PM.	ทำการ PM Server ประจำปี 2012	CAR NO : R2012-02	√		
	การบำรุงรักษาอุปกรณ์	ประจำปี (Server)					
6	ข้อกำหนด 3.2.5	> ไม่มีระเบียบปฏิบัติการทำลายอุปกรณ์	จัดทำระเบียบปฏิบัติการทำลาย	1. ทำลำดับขั้นตอนในการขออนุมัติทำลาย		√	
	การกำจัดอุปกรณ์และ การนำ	> ไม่มีระบบการขออนุมัติทำลาย	อุปกรณ์	2. จัดทำแบบฟอร์มการขออนุมัติทำลาย			
	อุปกรณ์กลับไปใช้ใหม่			อุปกรณ์สารสนเทศ			
				(Plan : 30/07/2555)			
7	ข้อกำหนด 4.1.1, 4.1.2	ไม่มีการทบทวน WI. ด้านงาน IT.	กำหนดให้มีการทบทวน WI. งานด้าน IT	ทบทวน WI. งานด้าน IT ประจำปี 2012		√	
	ขั้นตอนการปฏิบัติงานอย่างเป็น		เป็นประจำทุกปี	(Plan : 30/10/2555)			
	ลายลักษณ์อักษร						
8	ข้อกำหนด 4.3.2	ไม่มีระเบียบและ เอกสารการตรวจ	จัดให้มีระบบและกำหนดเกณฑ์ในการ	1. จัดทำเอกสารแบบฟอร์มการตรวจรับ		√	
	การตรวจรับระบบ	รับ Hardware	ตรวจรับ ระบบสารสนเทศทางด้าน	Hardware โดยกำหนดกรอบให้ใช้เฉพาะ			
			Hardware	ที่มีราคาสูง หรือระบบสำคัญๆ			
				(Plan : 30/07/2555)			

ภาคผนวก ฉ

Corrective Action Request (System)

LSD

Corrective Action Request (System)

Form. No. : LSD_F004
Edit : 1

CAR No. : _____
(หมายเลข CAR)

Information Risk Management for Data Security

Issue by Auditor : _____ **EMP.Code :** _____ **Issue date :** _____
(ผู้ออก CAR) (รหัสพนักงาน) (วันที่ออก)

Audit plan : _____ **Audit Time :** _____
(หมายเลขแผนการตรวจ) (การตรวจครั้งที่)

Area NC ; (พื้นที่ที่พบข้อบกพร่อง)
❑ SC Div. Sect. _____ ❑ PS Div. Sect. _____
❑ ADM Div. Sect. _____ ❑ Other Sect. _____

Level : VH. H. M.
(ระดับ CAR)

Type of CAR : (ประเภท CAR)
❑ Internal Audit
❑ Other NC (ระบุ) _____

Requirement Clause : _____
(ข้อกำหนดที่เกี่ยวข้อง)
Document No : _____
(เอกสารที่เกี่ยวข้อง)

Auditor

1 **Content of Non-conformity** (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

Due date (กำหนดแล้วเสร็จวันที่) :	Responsible action : (ผู้รับผิดชอบแก้ไข)	Checking by (ผู้ตรวจสอบการแก้ไข / IT Group. GL.)	Approval by (ตัวแทนฝ่ายบริหาร / HRM.Mgr. อนุมัติ)
_____ / _____ / _____			

Auditee

2 **Analysis root cause** (การวิเคราะห์หาสาเหตุ)

3 **Take Action** (การแก้ไข) | MGR./GL. Action approve (อนุมัติการแก้ไข โดยผู้จัดการ)

Action for re-occure (การป้องกันการเกิดซ้ำ)

Extension CAR : (ขอต่ออายุ CAR) Extension No. : _____ (หมายเลขเอกสารขอต่ออายุ) Extension to date (ขอต่ออายุถึงวันที่) _____

Auditor

4 **Follow up record** (ผลการติดตามการแก้ไขและป้องกัน) :

❑ Finished (close) (ทำการแก้ไขแล้วเสร็จ)

❑ can not close (ไม่สามารถทำการปิด CAR)

Efficiency of implementation (ติดตามผลหลังการดำเนินการแก้ไข)

Evidence (หลักฐานในการแก้ไข)

Because

❍ In case CAR expired re-issue CAR No. : _____
(ออก CAR ซ้ำ ในกรณีที่เกินกำหนดเสร็จ)

Auditor follow up (ผู้ติดตามการแก้ไข)	Approved by : (อนุมัติการติดตามการแก้ไข โดยตัวแทนฝ่ายบริหาร / HRM Mgr.)
Date : ____/____/____	Date : ____/____/____

Lumphun Shindengen Co.,Ltd.

ภาคผนวก ช

แบบฟอร์มแจ้งความเสี่ยงด้านความปลอดภัยของข้อมูล (Notify Risk Data Security)

LSD

แบบฟอร์มแจ้งความเสี่ยงด้าน ความปลอดภัยของข้อมูล

(Notify Risk Data Security)

Form. No. : LSD_F005
Edit : 1

Notified No. : _____

Annunciator

○ **Information Risk Management for Data Security**

Issue by Annunciator : _____ (ผู้แจ้งปัญหา) **EMP.Code :** _____ (รหัสพนักงาน) **Issue date :** _____ (วันที่ออก)

Area NC ; (พื้นที่ที่พบข้อบกพร่อง)
❑ SC Div. Sect. _____ ❑ PS Div. Sect. _____
❑ ADM Div. Sect. _____ ❑ Other Sect. _____

Requirement Clause : _____ (ข้อกำหนดที่เกี่ยวข้อง)

Document No : _____ (เอกสารที่เกี่ยวข้อง)

1 **การวิเคราะห์ความเสี่ยง (Risk Analysis)**

Content of Non-conformity (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

IT Group.

2 **การประมาณความเสี่ยง (Risk Estimation)**

Level : (ระดับ ความเสี่ยง) VH | H. | M. | L. | VL

3 **Take Action (การแก้ไข)**

CAR.	Plan / Edit	Acceptable

Assessors
(ผู้ประมาณค่าความเสี่ยง / IT Group. GL.)

หมายเหตุ

Due date (กำหนดเสร็จวันที่) : ____/____/____ ⇨ Responsible action : (ผู้รับผิดชอบแก้ไข) ⇨ Annunciator Acknowledge : (ผู้แจ้งรับทราบผล) ⇨ Approval by (ตัวแทนฝ่ายบริหาร/ HRM.Mgr. อนุมัติ)

Lumphun Shindengen Co.,Ltd.

ภาคผนวก ฌ

คู่มือการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลระบบสารสนเทศ 2555

Lumphun Shindengen Co., Ltd.

คู่มือ
การบริหารความเสี่ยง ด้านความปลอดภัยของข้อมูล
ระบบสารสนเทศ
2555

- ผู้จัดทำ(Editor)

  Mr. Amnaj Pongklang

- หน่วยงานรับผิดชอบ(Responsible)

  HRM Section

บทนำ

จากสภาวะเศรษฐกิจของโลกในปัจจุบันที่มีการแข่งขันกันอย่างรุนแรงและมีแนวโน้มที่จะเพิ่มสูงขึ้นเรื่อย ๆ นั้น ทำให้องค์กรภาคธุรกิจต่างพยายามสร้างความได้เปรียบในด้านการแข่งขัน และด้านประสิทธิภาพของต้นทุนอยู่ตลอดเวลา ทำให้ข้อมูลข่าวสารกลายเป็นหัวใจสำคัญในการทำธุรกิจในยุคนี้ โดยหลายองค์กรได้นำเทคโนโลยีสารสนเทศมาช่วยจัดเก็บข้อมูล เพื่อใช้ใน การขับเคลื่อนการเปลี่ยนแปลงกระบวนการทำงานที่เกิดขึ้นในองค์กร เพื่อให้มีประสิทธิภาพมากขึ้น และสร้างความได้เปรียบในด้านการแข่งขัน

สิ่งเหล่านี้ทำให้องค์กรต่าง ๆ มองเห็นความสำคัญของสารสนเทศ (Information) และเทคโนโลยีสารสนเทศ (Information Technology) ในองค์กร อันถือได้ว่าเป็นสินทรัพย์ที่มีค่ายิ่ง โดยเฉพาะในโลกของการแข่งขันที่รุนแรง ผู้บริหารจะให้ความสำคัญและความคาดหวังกับเทคโนโลยีสารสนเทศมากยิ่งขึ้นโดยเฉพาะการตอบสนองที่รวดเร็วต่อเนื่องตลอดเวลา รวมถึงมีคุณภาพสามารถใช้งานได้หลากหลาย และสะดวกต่อการใช้งาน โดยใช้เวลาน้อยลง เพิ่มระดับการบริการให้ดียิ่งขึ้น และมีต้นทุนที่ต่ำลง

จะเห็นได้ว่าข้อมูล สารสนเทศนั้นมีความสำคัญกับ บริษัท ลำพูนซิงเดนเก็น จำกัด เป็นอย่างมาก โดยบริษัทนั้นมีความต้องการใช้ข้อมูล สารสนเทศอย่างต่อเนื่องตลอดเวลา และบริษัทจะได้รับผลกระทบอย่างมาก หากการให้บริการข้อมูล สารสนเทศเกิดหยุดชะงัก ข้อมูลเสียหาย หรือรั่วไหลไปยังบริษัทคู่แข่ง ทำให้การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล เป็นเรื่องที่สำคัญเรื่องหนึ่งที่บริษัทควรจะพิจารณาจัดการบริหารอย่างเป็นระบบ และอ้างอิง ตามมาตรฐานสากลที่มีการกำหนดกรอบการปฏิบัติไว้อย่างชัดเจน รวมไปถึงการ พิจราณาปรับปรุงกระบวนการจัดการระบบสารสนเทศด้านความปลอดภัยของข้อมูล โดยนำเอามาตรฐานการบริหารจัดการด้านเทคโนโลยีสารสนเทศมาแก้ปัญหา หรือสร้างระบบป้องกันความเสี่ยง เพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ดังนั้น การดำเนินการในเรื่อง ***"การบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล"*** จะทำให้บริษัทสามารถมีระบบสารสนเทศในการขับเคลื่อนธุรกิจ โดยมีข้อมูลสารสนเทศที่ถูกต้อง ปลอดภัย มีระบบ และเทคโนโลยีสารสนเทศที่สามารถให้บริการได้ อย่างต่อเนื่องตลอดเวลา

บทที่ 1

มาตรฐานที่ใช้อ้างอิง

มาตรฐานที่นำมาปรับใช้ในการจัดทำระบบ การบริหารจัดการความเสี่ยงด้าน ความปลอดภัยของข้อมูลในครั้งนี้คือ มาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 27002:2005 ซึ่งเป็นมาตรฐานสากลด้านการบริหารความมั่นคงของข้อมูล ซึ่งเน้นความสำคัญที่ "ระบบการบริหารจัดการ" (Management System) โดยมีข้อกำหนดต่าง ๆ ที่องค์กรพึงปฏิบัติในการรักษาความมั่นคงของข้อมูล เพื่อปกป้องข้อมูลกระบวนการทางธุรกิจ และทรัพย์สินด้านสารสนเทศ ที่สำคัญให้พ้นจากภัยคุกคาม และความเสี่ยงในรูปแบบต่าง ๆ รวมถึงกำหนดให้มีการจัดทำแผนรับมือเหตุฉุกเฉินที่อาจเกิดขึ้น เพื่อลดความสูญเสีย และคงไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

1) มาตรฐาน ISO/IEC 27001:2005 (Information Security Management System : ISMS)

ISO/IEC 27001:2005 (Information Security Management System : ISMS) กล่าวถึง ข้อกำหนดสำหรับใช้เป็นเกณฑ์ในการตรวจรับรองความมีมาตรฐานของ "ระบบบริหารความมั่นคงของข้อมูล" (Information Security Management Systems : ISMS) โดยมีรายละเอียดนับตั้งแต่การริเริ่มทำระบบการปฏิบัติ ใช้งาน การทบทวน การปรับปรุงอย่างต่อเนื่อง ซึ่งสอดคล้องกับแนวคิดของหลักการ PDCA (Plan-Do-Check-Act) นั่นเอง ทั้งนี้ ระบบ ISMS ที่จัดตั้งขึ้นนั้น จะต้องอ้างอิงตามหัวข้อของการควบคุมด้านความมั่นคงของข้อมูล 133 หัวข้อในมาตรฐาน ISO 27002 ตามความเหมาะสมด้วย

เนื้อหาของมาตรฐาน ISO 27001:2005 จะเกี่ยวข้องกับการจัดตั้งและปฏิบัติใช้งาน "ระบบบริหารความมั่นคงของข้อมูล" (Information Security Management Systems : ISMS) ขึ้นในองค์กร ซึ่งแนวคิดของมาตรฐานส่วนนี้จะเป็นแนวทางสำคัญ สำหรับองค์กรที่ต้องการนำระบบ ISMS ไปใช้ในการปกป้องข้อมูล กระบวนการธุรกิจ และทรัพย์สินด้านสารสนเทศที่สำคัญขององค์กร เนื้อหาของมาตรฐาน ISO 27001:2005 แบ่งออกเป็น 8 ส่วน ดังนี้

(1) ขอบเขต (Scope)

(2) มาตรฐานอ้างอิง (Normative Reference)

(3) คำจำกัดความและนิยาม (Terms and Definitions)

(4) ระบบบริหารความมั่นคงของข้อมูล (Information Security Management System)

(5) หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management Responsibility)

(6) การตรวจประเมินการบริหารความมั่นคงของข้อมูลภายใน (Internal ISMS Audit)

(7) การทบทวนการบริหารความมั่นคงของข้อมูล (Management Review of the ISMS)

(8) การปรับปรุงการบริหารความมั่นคงของข้อมูล (ISMS Improvement)

มาตรฐานนี้ได้ถูกจัดทำขึ้น โดยยึดตามแนวคิดของหลักการ PDCA (Plan-Do-Check-Act) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาขึ้นอย่างต่อเนื่อง (Continuous Improvement) เริ่มต้นตั้งแต่การจัดตั้ง (Establish) การนำระบบไปใช้ (Implement) การดำเนินงาน (Operate) การติดตามและวัดผล (Monitor) การทบทวน (Review) การบำรุงรักษาระบบ (Maintain) และการปรับปรุงพัฒนาระบบให้ดียิ่งขึ้น (Improve) ซึ่งสามารถอธิบายได้ดังภาพที่ 1

ภาพที่ 1 แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตาม ขั้นตอนPlan-Do-Check-Act

2) มาตรฐาน ISO/IEC 17799:2005 Information Technology Security Techniques Code of Practice for Information Security Management

มาตรฐาน ISO/IEC 17799 เป็นมาตรฐานที่กล่าวถึงเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบ โดยแบ่งหัวข้อหลักที่เกี่ยวข้องกับระบบ และให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการ หรือใช้วิธีการที่มีความมั่นคงปลอดภัยเพียงพอ หรือเหมาะสมตามที่องค์กรได้ประเมินไว้ ซึ่งหัวข้อสำคัญ หรือ 11 โดเมนหลักในมาตรฐานดังกล่าวมีดังนี้

(1) นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

(2) โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

(3) การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)

(4) ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

(5) การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

(6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and Operations Management)

(7) การควบคุมการเข้าถึง (Access Control)

(8) การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)

(9) การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information Security Incident Management)

(10) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)

(11) การปฏิบัติตามข้อกำหนด (Compliance)

จาก 11 โดเมนหลักในมาตรฐาน ISO/IEC 17799 ที่ได้กล่าวมา ได้ถูกนำมาจัดเป็นวิธีปฏิบัติที่จะนำไปสู่ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กร โดยสามารถสรุปเป็นขั้นตอนการดำเนินงานได้ดังนี้

(1) การประเมินความเสี่ยง (Risk Assessment)

การวิเคราะห์ความเสี่ยงประกอบด้วย 3 กระบวนการ คือ

กระบวนการที่ 1 การชี้ระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงปัญหา สิ่งคุกคาม และความไม่แน่นอนที่องค์กรต้องเผชิญที่จะส่งผลกระทบต่อข้อมูลสารสนเทศ ทั้ง 3 ด้าน

กระบวนการที่ 2 ลักษณะรายละเอียดของความเสี่ยง (Description of Risk) เป็นการระบุ ขยายความ รายละเอียด และลักษณะของความเสี่ยงนั้นๆ

กระบวนการที่ 3 การประมาณความเสี่ยง (Risk Estimation) เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุว่ามีโอกาสมากน้อยเพียงไร และผลที่ติดตามมา มีความรุนแรงหรือเสียหายมากน้อยเพียงใด โดยแบ่งระดับ โอกาสการเกิดความเสี่ยง และความรุนแรงของความเสี่ยงไว้ 3 ระดับ คือ สูง ปานกลาง และน้อย

(2) ประเมินค่าความเสี่ยง (Risk Evaluation) เป็นการประเมินค่าความเสี่ยงโดยการเปรียบเทียบกับหลักเกณฑ์ความเสี่ยงที่ยอมรับได้ หรือหลักเกณฑ์ยอมรับความเสี่ยง เพื่อประกอบการตัดสินใจว่าจะบำบัดความเสี่ยงนั้นหรือไม่

(3) การรายงานผลการวิเคราะห์ความเสี่ยง (Risk Reporting) เป็นเอกสารผลการประเมินความเสี่ยง เพื่อรายงานต่อผู้บริหารให้ทราบถึงความเสี่ยงที่องค์กรเผชิญอยู่

(4) กระบวนการบรรเทาและควบคุมความเสี่ยง (Risk Mitigation and Control) เป็นการเสนอแผนงาน วิธีการ บรรเทา ป้องกัน และควบคุมความเสี่ยง และดำเนินการตามวิธีการที่ผู้บริหารเห็นชอบและอนุมัติ

(5) การรายงานความเสี่ยงตกค้าง (Residual Risk Reporting) เป็นรายงานความเสี่ยงที่ยังไม่สามารถป้องกันหรือแก้ไขได้ เพื่อเป็นข้อมูลในการวางแผนระยะยาวต่อไป

(6) การเฝ้าสังเกต (Monitoring) จัดทำแผนการตรวจสอบภายใน(Internal Audit) เพื่อตรวจสอบว่าแผนการป้องกันและควบคุมความเสี่ยงนั้น ผู้ปฏิบัติได้ปฏิบัติตามมาตรฐาน หรือวิธีการที่ได้ประกาศไว้อย่างถูกต้องและสม่ำเสมอหรือไม่

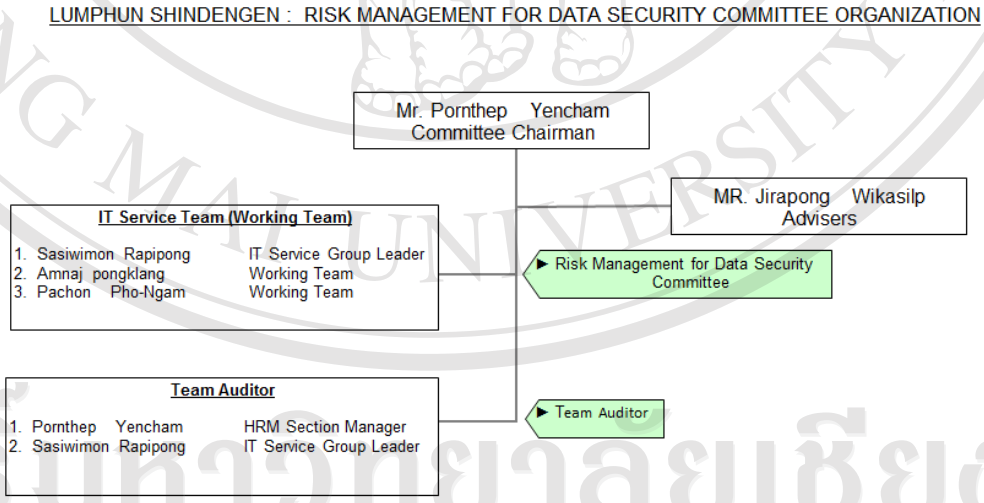
ดังนั้น จึงสรุปได้ว่า ความแตกต่างของมาตรฐาน ISO/IEC 27001 และมาตรฐาน ISO/IEC 17799 คือ มาตรฐาน ISO/IEC 27001 จะเน้นเรื่องข้อกำหนดใน การจัดทำระบบ ISMS ให้กับองค์กรตามขั้นตอน Plan-Do-Check-Act และใช้แนวทางในการประเมินความเสี่ยงมาประกอบการพิจารณาเพื่อหาวิธีการหรือมาตรการที่เหมาะสม ส่วนมาตรฐาน ISO/IEC 17799 จะเน้นเรื่องวิธีปฏิบัติที่จะนำไปสู่ระบบ ISMS ที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามมาตรฐาน ISO/IEC 27001 กำหนดไว้ด้วย

บทที่ 2

กระบวนการจัดทำระบบ การบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล

กระบวนการจัดทำระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลของ บริษัทลำพูน ซิงเด็นเก็น จำกัด มีขั้นตอนดังต่อไปนี้

1. จัดตั้งคณะทำงานด้านบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล ประจำปี 2012 โดยแบ่งออกเป็น 2 ชุดคือ ชุดที่1 คณะกรรมการตรวจสอบความเสี่ยงด้านความปลอดภัยของข้อมูล (Team Auditor) ชุดที่ 2 คณะทำงาน ด้านการจัดการความเสี่ยงด้านความปลอดภัยของข้อมูล (Working Team) โดยมีหน้าที่ในการหาแนวทางการแก้ไขหรือควบคุม ป้องกันความเสี่ยงที่ตรวจพบ ให้อยู่ในระดับที่ยอมรับได้หรือไม่มีความเสี่ยงนั้นๆอีก เพื่อไม่ให้เกิดผลกระทบกับการดำเนินงานของบริษัท โดยโครงสร้างของคณะทำงานทั้ง 2 ชุด ดังที่แสดงในภาพที่ 2 Risk Management For Data Security Committee Organization



ภาพที่ 2 Risk Management For Data Security Committee Organization

2. จัดเตรียมเอกสาร แบบฟอร์มต่างๆที่ใช้จะสำหรับการตรวจสอบและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล โดยมีรายละเอียดของเอกสารดังนี้

   1) Information Risk Management for Data Security Systems Requirements เป็นการนำเอา Requirements ของ ISO 27001:2005 มาบรรจุไว้เพื่อใช้เป็นกรอบการดำเนินการของระบบที่จัดทำขึ้น โดยสามารถดูรายละเอียดเพิ่มได้ที่เอกสารหมายเลข LSD_D001

   2) Internal Audit Manual เป็นแนวทางปฏิบัติ และตรวจสอบ ซึ่งเอกสารฉบับนี้จะระบุถึงรายละเอียดแนวทางในการปฏิบัติ ให้ถูกต้องตามข้อกำหนดในแต่ละข้อ โดยสามารถดูรายละเอียดเพิ่มได้ที่เอกสารหมายเลข LSD_D002

   3) Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง) เป็นเอกสารที่ระบุถึงกฎเกณฑ์ในการประมาณความเสี่ยงที่ตรวจพบ เพื่อนำไปจัดลำดับความสำคัญ และนำไปสู่การจัดลลำดับการแก้ไขหรือมาตรการควบคุมความเสี่ยง โดยสามารถดูรายละเอียดเพิ่มได้ที่เอกสารหมายเลข LSD_D003

   4) แบบฟอร์มที่ใช้ในกระบวนการตรวจและ ประเมินความเสี่ยงมีดังนี้

      4.1 INFORMATION RISK MANAGEMENT FOR DATA SECURITY REQUIREMENT & AUDIT SCOPE MATRIX เป็นฟอร์มแรกในกระบวนการวางแผนการตรวจและ ประเมินความเสี่ยง ด้านความปลอดภัยของข้อมูล ซึ่งเป็นฟอร์มที่ใช้สำหรับการเชื่อมโยงความสำพันธ์ ระหว่างขอบเขตข้อมูล ของการตรวจในแต่ละครั้ง กับข้อกำหนดตามมาตรฐานของระบบ บริหารจัดการความเสี่ยงด้าน ความปลอดภัยของข้อมูล โดยสามารถดูรายละเอียดเพิ่มได้ที่ฟอร์มหมายเลข LSD_F001

      4.2 Internal Audit Checklist เป็นฟอร์มที่เชื่อมโยงความสำพันธ์ ระหว่างขอบเขตข้อมูล ของการตรวจในแต่ละครั้ง กับข้อกำหนดตามมาตรฐานของระบบบริหารจัดการความเสี่ยงด้าน ความปลอดภัยของข้อมูลเช่นกัน แต่จะมีการเพิ่มในส่วนของ Audit Question ซึ่งเป็นแนวทาง คำถามหรือ ขอสังเกตในการตรวจที่สอดคล้องกับข้อกำหนด โดยสามารถดูรายละเอียดเพิ่มได้ที่ฟอร์มหมายเลข LSD_F002

4.3 Internal Audit Report เป็นฟอร์มที่ใช้สำหรับประมาณระดับความเสี่ยงที่ตรวจพบ โดยจะใช้งานร่วมกับเอกสาร Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง): LSD_D003 โดยสามารถดูรายละเอียดเพิ่มได้ที่ฟอร์มหมายเลข LSD_F003

4.4 Corrective Action Request (CAR) เป็นเอกสารที่ใช้สำหรับการ ร้องข้อให้มีการ Action ในกรณีที่ความเสี่ยงที่ตรวจพบ และถูกประเมินว่าอยู่ในระดับ M คือมีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง), H คือ มีความเสี่ยงและผลกระทบ (เสี่ยง)และ VH คือ มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก) โดยสามารถดูรายละเอียดเพิ่มได้ที่ฟอร์มหมายเลข LSD_F004

บทที่ 3

กระบวนตรวจสอบและประเมินความเสี่ยง

กระบวนการตรวจสอบและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล บริษัทลำพูนซิงเด็นเก็น จำกัด มีกระบวนการดังนี้

ขั้นตอนที่ 1 การกำหนดขอบเขตการตรวจ (Audit Scope)

ในการตรวจครั้งนี้ได้กำหนดขอบเขตการตรวจ (Audit Scope) ไว้ 7 หัวข้อดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy)
2. ระบบเอกสารส่วนกลาง (File Sharing : LSD DATA SERVER, LSD PS SERVER)
3. Database Server จำนวน 4 Server (ERP. System, MRP. System, HRMS, DB Systems)
4. Active Directory Database
5. ระบบข้อมูลสนับสนุน (Service Support Systems : Mail Server, Web Server)
6. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (ALL LSD SERVER)
7. ระบบทางด้านฮาร์ดแวร์ที่เกี่ยวข้องกับข้อมูลโดยตรง (Network Systems)

ขั้นตอนที่ 2 การวางแผนการตรวจ

นำขอบเขตการตรวจที่กำหนดขึ้นมาทำการวางแผนการตรวจโดยสร้างเป็น INFORMATION RISK MANAGEMENT FOR DATA SECURITY REQUIREMENT & AUDIT SCOPE MATRIX โดยใช้ฟอร์ม LSD_F001 จากนั้นก็สร้างเป็น Internal Audit Checklist ในการตรวจครั้งนี้โดยใช้ ฟอร์ม LSD_F002

ขั้นตอนที่ 3 การประชุมชี้แจ้งขอบเขตการตรวจ

การประชุมครั้งนี้มีวัตถุประสงค์ 2 อย่างคือ

1. Auditor Training เนื่องจากเป็นระบบใหม่ที่มีการนำมาใช้ในบริษัทเป็นครั้งแรก จึงต้องมีความจำเป็นต้องทำการอบรมชี้แจง รายละเอียดของระบบให้ Auditor ได้เข้าใจ

2. Audit Opening ถือเป็นการเปิดการตรวจสอบอย่างเป็นทางการ โดยเป็นการชี้แจงถึง ขอบเขตในการตรวจครั้งนี้และถือเป็นการพูดคุยเพื่อปรับมุมมองของ Auditor แต่ละคนให้มีมุมมองในการตรวจและมุ่งไปในประเด็นและแนวทางเดียวกัน

ขั้นตอนที่ 4 การตรวจสอบภายในระบบการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูล

ในการตรวจแต่ละครั้งผู้ตรวจ (Auditor) จะยึดเอา Internal Audit Checklist เป็นแนวทางในการตรวจเพื่อควบคุมให้การตรวจครั้งนั้นๆ อยู่ในประเด็นที่กำหนดไว้ในขอบเขต โดยมีขั้นตอนการตรวจดังนี้

1. ผู้ตรวจทำการบันทึก ข้อบกพร่องหรือความเสี่ยงที่ตรวจพบ ลงใน Internal Audit Report ฟอร์ม LSD_F003 ในช่องของ Risk Identification (บ่งชี้ความเสี่ยง) และ Risk Description (รายละเอียดความเสี่ยง)
2. ผู้ตรวจนำข้อบกพร่องหรือความเสี่ยงที่ตรวจพบ ที่บันทึกลงในฟอร์ม LSD_F003 มาเข้าประชุมร่วม ระหว่างผู้ตรวจ(Auditor) กับผู้รับตรวจ (Auditee) เพื่อทำการประมาณค่าความเสี่ยงที่ตรวจพบ
3. เมื่อทำการประมาณค่าความเสี่ยงที่ตรวจพบ แล้วให้พื้นที่ผู้รับผิดชอบ นำข้อมูลที่ได้ไปทำการ สรุปเป็นรายงานการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลต่อไป

บทที่ 4

รายงานการบริหารและ จัดการความเสี่ยงด้าน ความปลอดภัยของข้อมูล

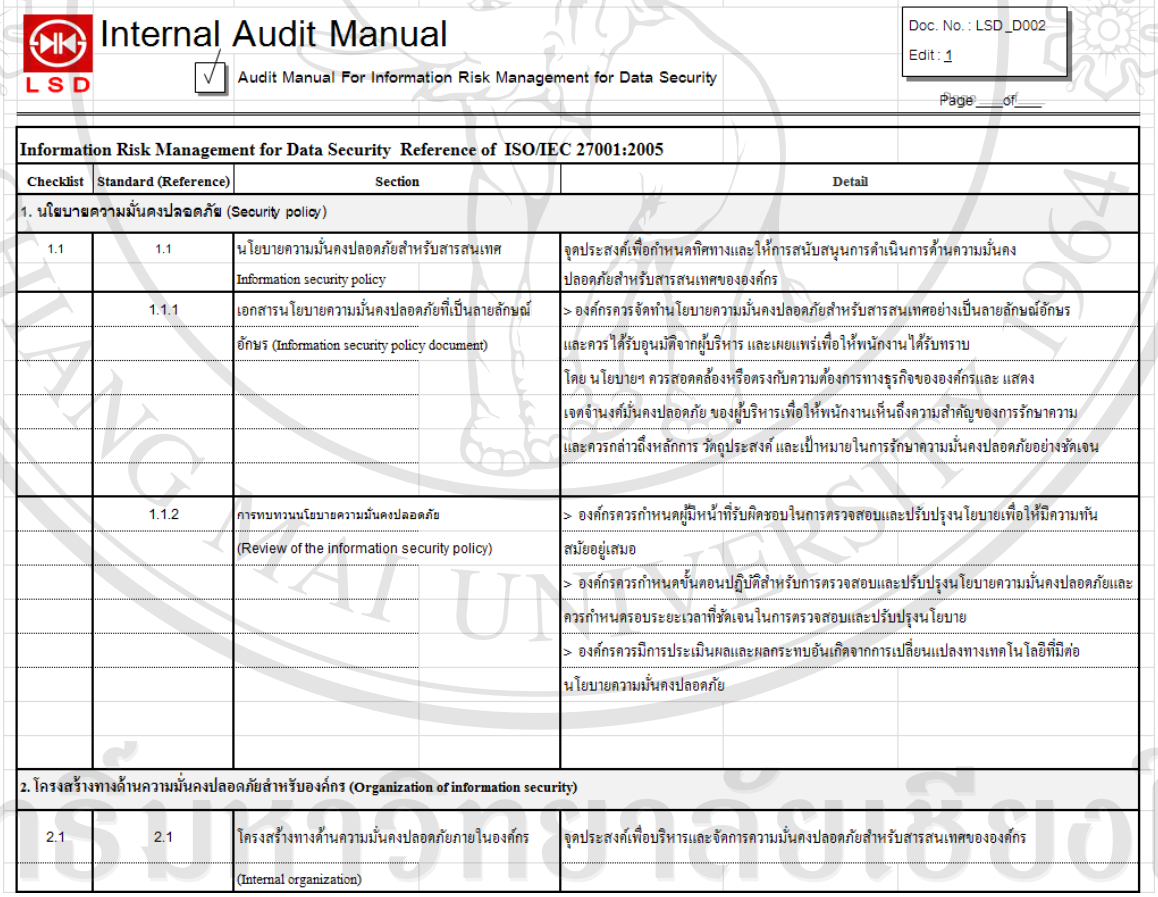
ผู้รับผิดชอบ แผนก HRM กลุ่มงาน IT Service ได้ทำการสรุปเป็นรายงานการบริหารความเสี่ยงด้าน ความปลอดภัยของข้อมูล โดยรายละเอียดแสดง ดังรายงานที่แนบไว้ท้ายคู่มือฉบับนี้

บทที่ 5

ตัวอย่างเอกสารและแบบฟอร์ม

เอกสารและแบบฟอร์ม ที่มีใช้งานในระบบ การบริหารความเสี่ยง ด้านความปลอดภัยของข้อมูล มีรายละเอียดดังตัวอย่างต่อไปนี้

1. LSD_D001 : Information Risk Management for Data Security Systems Requirements
2. LSD_D002 : Internal Audit Manual



LSD

Internal Audit Manual

Audit Manual For Information Risk Management for Data Security

Doc. No. : LSD_D002
Edit : 1
Page ___of___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005			
Checklist	**Standard (Reference)**	**Section**	**Detail**
1. นโยบายความมั่นคงปลอดภัย (Security policy)			
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ Information security policy	จุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร
	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	> องค์กรควรจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร และควรได้รับอนุมัติจากผู้บริหาร และเผยแพร่เพื่อให้พนักงานได้รับทราบ โดย นโยบายฯ ควรสอดคล้องหรือตรงกับความต้องการทางธุรกิจขององค์กรและ แสดงเจตจำนงค์มั่นคงปลอดภัย ของผู้บริหารเพื่อให้พนักงานเห็นถึงความสำคัญของการรักษาความและควรกล่าวถึงหลักการ วัตถุประสงค์ และเป้าหมายในการรักษาความมั่นคงปลอดภัยอย่างชัดเจน
	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	> องค์กรควรกำหนดผู้มีหน้าที่รับผิดชอบในการตรวจสอบและปรับปรุงนโยบายเพื่อให้มีความทันสมัยอยู่เสมอ > องค์กรควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบและปรับปรุงนโยบายความมั่นคงปลอดภัยและควรกำหนดรอบระยะเวลาที่ชัดเจนในการตรวจสอบและปรับปรุงนโยบาย > องค์กรควรมีการประเมินผลและผลกระทบอันเกิดจากการเปลี่ยนแปลงทางเทคโนโลยีที่มีต่อนโยบายความมั่นคงปลอดภัย
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)			
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)	จุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

3. LSD_D003 : Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง)

Doc. No. : LSD_D003
Edit : 1

Risk Estimation (ตารางเมตริกซ์การประมาณความเสี่ยง)

ความรุนแรงและ ผลกระทบของความเสี่ยง (Impact)	โอกาสที่ความเสี่ยงจะเกิดขึ้น (Likelihood)				
	น้อยมาก (1),(VL)	น้อย (2), (V)	ปานกลาง (3), (M)	บ่อย (4), (H)	บ่อยมาก (5), (VH)
รุนแรงมาก (20) = VH					
รุนแรง (15) = V					
ปานกลาง (10) = M					
น้อย (5) = V					
น้อยมาก (1) = VL					

Risk Assessment Matrix

VH = มีความเสี่ยงและผลกระทบมาก (เสี่ยงมาก)	20	40	60	80	100
H = มีความเสี่ยงและผลกระทบ (เสี่ยง)	15	30	45	60	75
M = มีความเสี่ยงและผลกระทบปานกลาง (ปานกลาง)	10	20	30	40	50
L = มีความเสี่ยงและผลกระทบต่ำ (ต่ำ)	5	10	15	20	25
VL = มีความเสี่ยงและผลกระทบต่ำมาก (ต่ำมาก)	1	2	3	4	5

4. LSD_F001 : INFORMATION RISK MANAGEMENT FOR DATA SECURITY REQUIREMENT & AUDIT SCOPE MATRIX

INFORMATION RISK MANAGEMENT FOR DATA SECURITY REQUIREMENT & AUDIT SCOPE MATRIX

Form. No. : LSD_F001
Edit : 1 Eff.date :

Requirement	1. นโยบายความมั่นคงปลอดภัย (Security policy)	2. ระบบแลกสารส่วนกลาง (File Sharing : LSD DATA SERVER, LSD PS SERVER)	3. Database Server จำนวน 4 Server (ERP. System, MRP. System, HRMS, DB Systems)	4. Active Directory Database	5. ระบบห้องคอมพิวเตอร์แม่ข่าย (Service Support Systems : Mail Server, Web Server)	6. ระบบเครือข่ายสายสัญญาณที่เกี่ยวข้องกับห้องคอมพิวเตอร์แม่ข่าย (ALL LSD SERVER)	7. ระบบเครือข่ายสายสัญญาณที่เกี่ยวข้องกับห้องคอมพิวเตอร์แม่ข่าย (Network Systems)	
1. นโยบายความมั่นคงปลอดภัย (Security policy)								
1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information Security Policy)	●							
1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	●							
1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	●							
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)								
2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)								
2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการ ทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	●							

5. LSD_F002 : Internal Audit Checklist

LSD

Internal Audit Checklist

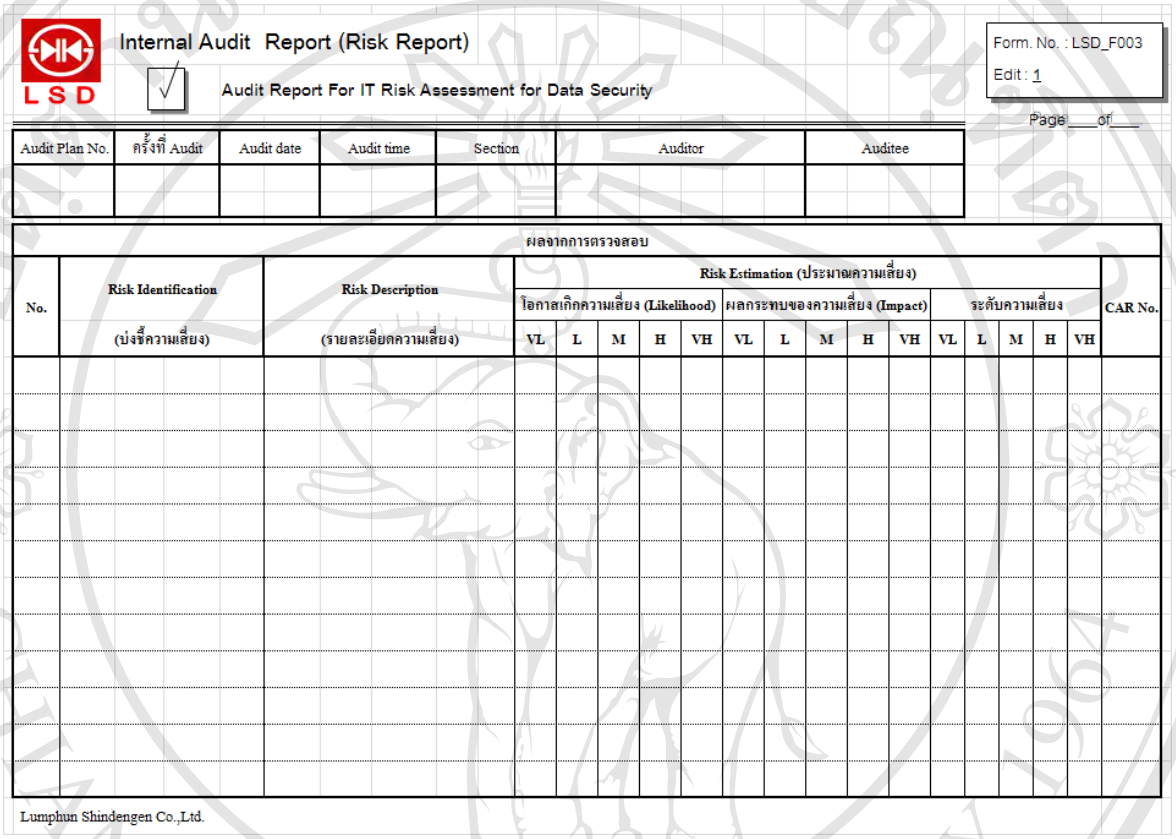
☑ Audit Checklist For Information Risk Management for Data Security

Form. No. : LSD_F002
Edit : 1
Page ___ of ___

Information Risk Management for Data Security Reference of ISO/IEC 27001:2005

Checklist	Standard (Reference)	Section	Audit Question	Audit Scope	Findings (OK / NC)
1. นโยบายความมั่นคงปลอดภัย (Security policy)					
1.1	1.1	นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ Information security policy			
1.1.1	1.1.1	เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)	องค์กรมีนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากผู้บริหาร และ เผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
1.1.2	1.1.2	การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)	องค์กรมีการ ทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)					
2.1	2.1	โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)			
2.1.1	2.1.1	การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)	ผู้บริหาร มีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง รวมถึงการมอบหมายงานที่เหมาะสมต่อบุคลากร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.2	2.1.2	การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)	ผู้บริหาร มีการกำหนด ตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	
2.1.3	2.1.3	การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)	ผู้บริหาร มีการกำหนดหน้าที่ความรับผิดชอบของพนักงานใน การดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน หรือไม่	1. นโยบายความมั่นคงปลอดภัย (Security policy)	

6. LSD_F003 : Internal Audit Report



LSD

Internal Audit Report (Risk Report)

Audit Report For IT Risk Assessment for Data Security

Form. No. : LSD_F003
Edit : 1
Page ___ of ___

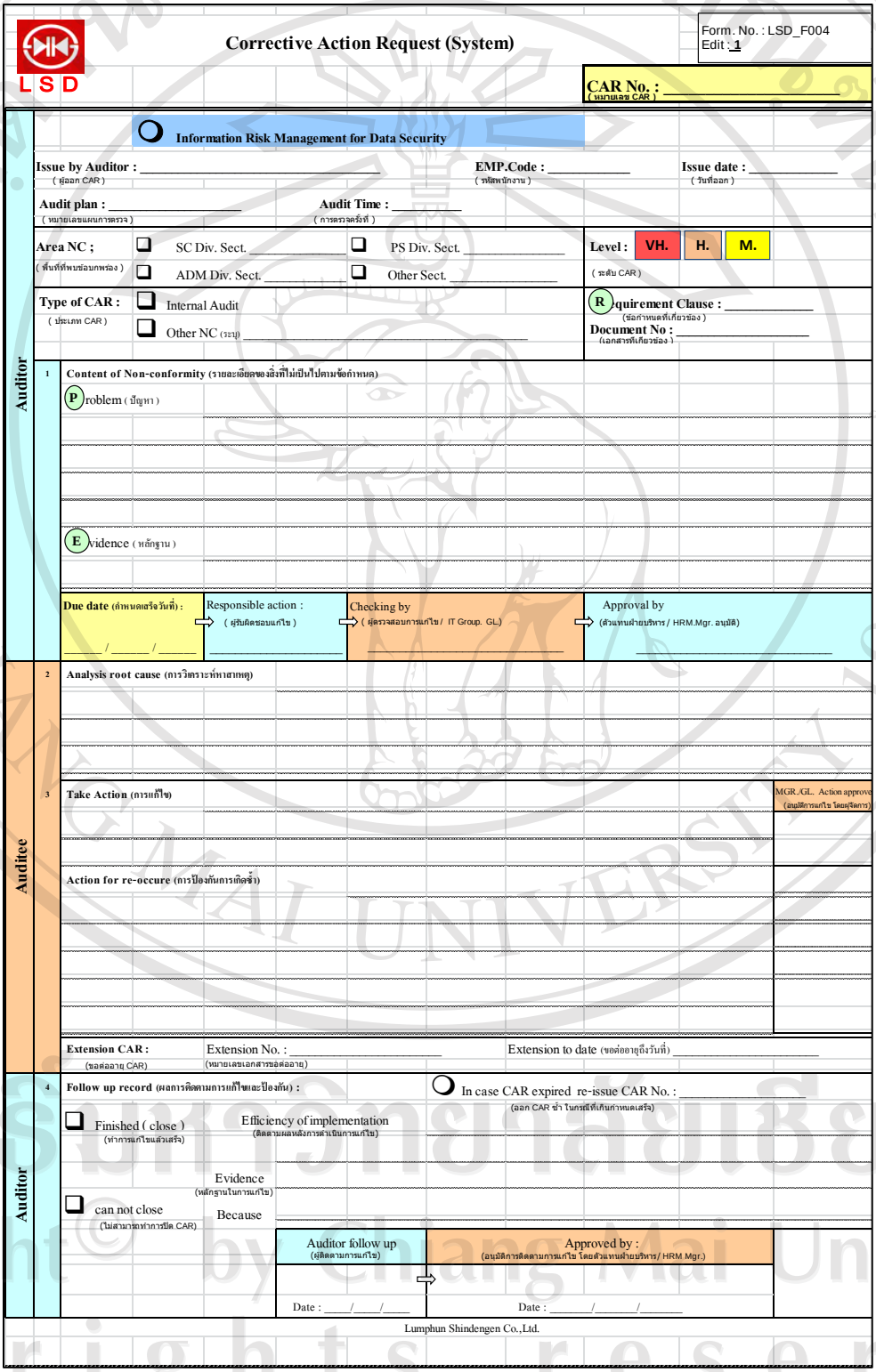
Audit Plan No.	ครั้งที่ Audit	Audit date	Audit time	Section	Auditor	Auditee

ผลจากการตรวจสอบ

No.	Risk Identification (บ่งชี้ความเสี่ยง)	Risk Description (รายละเอียดความเสี่ยง)	Risk Estimation (ประมาณความเสี่ยง)															CAR No.
			โอกาสเกิดความเสี่ยง (Likelihood)					ผลกระทบของความเสี่ยง (Impact)					ระดับความเสี่ยง					
			VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	

Lumphun Shindengen Co.,Ltd.

7. LSD_F004 : Corrective Action Request (CAR)



Corrective Action Request (System)

Form. No. : LSD_F004
Edit : 1

LSD

CAR No. : _____
(หมายเลข CAR)

Auditor

Information Risk Management for Data Security

Issue by Auditor : _____ (ผู้ออก CAR) **EMP.Code :** _____ (รหัสพนักงาน) **Issue date :** _____ (วันที่ออก)

Audit plan : _____ (หมายเลขแผนการตรวจ) **Audit Time :** _____ (การตรวจครั้งที่)

Area NC ; (พื้นที่ที่พบข้อบกพร่อง)
- SC Div. Sect. _____
- PS Div. Sect. _____
- ADM Div. Sect. _____
- Other Sect. _____

Level : VH. H. M. (ระดับ CAR)

Type of CAR : (ประเภท CAR)
- Internal Audit
- Other NC (ระบุ) _____

Requirement Clause : _____ (ข้อกำหนดที่เกี่ยวข้อง)
Document No : _____ (เอกสารที่เกี่ยวข้อง)

1 **Content of Non-conformity** (รายละเอียดของสิ่งที่ไม่เป็นไปตามข้อกำหนด)

Problem (ปัญหา)

Evidence (หลักฐาน)

Due date (กำหนดเสร็จวันที่) :	Responsible action : (ผู้รับผิดชอบแก้ไข)	Checking by (ผู้ตรวจสอบการแก้ไข / IT Group. GL.)	Approval by (ตัวแทนฝ่ายบริหาร / HRM.Mgr. อนุมัติ)
_____/_____/_____	_____	_____	_____

Auditee

2 **Analysis root cause** (การวิเคราะห์หาสาเหตุ)

3 **Take Action** (การแก้ไข) | MGR./GL. Action approve (อนุมัติการแก้ไข โดยผู้จัดการ)

Action for re-occure (การป้องกันการเกิดซ้ำ)

Extension CAR : (ขอต่ออายุ CAR) Extension No. : _____ (หมายเลขเอกสารขอต่ออายุ) Extension to date (ขอต่ออายุถึงวันที่) _____

Auditor

4 **Follow up record** (ผลการติดตามการแก้ไขและป้องกัน) :

In case CAR expired re-issue CAR No. : _____ (ออก CAR ซ้ำ ในกรณีที่เกินกำหนดเสร็จ)

- Finished (close) (ทำการแก้ไขแล้วเสร็จ)
- can not close (ไม่สามารถทำการปิด CAR)

Efficiency of implementation (ติดตามผลหลังการดำเนินการแก้ไข)

Evidence (หลักฐานในการแก้ไข)

Because

Auditor follow up (ผู้ติดตามการแก้ไข)	Approved by : (อนุมัติการติดตามการแก้ไข โดยตัวแทนฝ่ายบริหาร/ HRM.Mgr.)
Date : ____/____/____	Date : _____/_____/_____

Lumphun Shindengen Co.,Ltd.

ประวัติผู้เขียน

ชื่อ – สกุล นายอำนาจ พงษ์กลาง

วัน เดือน ปีเกิด 16 กันยายน 2522

ประวัติการศึกษา สำเร็จการศึกษาระดับปริญญาตรี ครุศาสตร์บัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีราชมงคล วิทยาเขต
ภาคพายัพ ปีการศึกษา 2547

ประสบการณ์ทำงาน พ.ศ. 2548 – ปัจจุบัน พนักงานบริษัท ลำพูนซิงเดนเก็น จำกัด
นิคมอุตสาหกรรม จังหวัดลำพูน ตำแหน่งวิศวกรคอมพิวเตอร์