การประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001: กรณีศึกษาบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน)

ธิดา ลิ่มทองวิรัตน์, ผู้ช่วยศาสตราจารย์ สุนีย์ ตฤณขจี
บัณฑิตวิทยาลัย สาขาวิชาการตรวจสอบภายใน
คณะบัญชี, มหาวิทยาลัยหอการค้าไทย
โทรศัพท์ : 089-1181973, E-mail : tida_lim@hotmail.com

บทคัดย่อ

การศึกษาค้นคว้าด้วยตนเอง เรื่อง การประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001: กรณีศึกษาบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) มีวัตถุประสงค์เพื่อศึกษาแนวทางเพื่อประเมินประสิทธิผลของระบบการควบคุมภายในสารสนเทศ เรื่องการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 อีกทั้งเพื่อวิเคราะห์ปัญหาอุปสรรค และจุดอ่อนในระบบการควบคุมภายในสารสนเทศรวมถึงเสนอแนะแนวทางการควบคุมที่มีประสิทธิภาพ รวมถึงเพื่อประเมินการปฏิบัติงานของพนักงานให้เป็นไปตามขั้นตอนมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ผลที่ได้จากการศึกษาพบว่า ในภาพรวมบริษัทมีการควบคุมภายในด้านสารสนเทศในระดับเพียงพอแล้ว โดยมีระดับการควบคุมที่ดี โดยบริษัทยังคงต้องให้ความสนใจในเรื่องที่ยังไม่ได้มีการปฏิบัติตามมาตรฐานในระดับที่เพียงพอ 3 เรื่องคือ เรื่องการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพสมบูรณ์ เรื่องการบันทึกเหตุการณ์ข้อผิดพลาด และเรื่องการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน ข้อเสนอแนะเกี่ยวกับการบำรุงรักษาอุปกรณ์คือ ควรเพิ่มกระบวนการควบคุมและการเก็บรักษาอุปกรณ์ รวมถึงกระบวนการซ่อมแซมและการบำรุงรักษาอุปกรณ์ ในเรื่องการบันทึกเหตุการณ์ข้อผิดพลาด ควรเพิ่มรายงานเหตุการณ์ที่เกิดขึ้น เพื่อจัดทำรายงานประจำสัปดาห์เสนอให้ต่อผู้บริหารทราบ และเรื่องการตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน ผู้ดูแลระบบต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

บทนำ

ปัจจุบันรูปแบบการทำงานขององค์กรเกือบทุกแห่งทั่วโลกมีการเปลี่ยนแปลงเป็นอย่างมาก ทั้งนี้ด้วยความก้าวหน้าของเทคโนโลยีส่งผลให้คอมพิวเตอร์ เทคโนโลยีสารสนเทศ และระบบต่าง ๆ เข้ามามีบทบาทสำคัญต่อกระบวนการทางธุรกิจอย่างหลีกเลี่ยงไม่ได้ ปรากฏการณ์เช่นนี้ส่งผลให้การดำเนินธุรกิจขององค์กรมีความจำเป็นที่จะต้องพึ่งพาระบบเทคโนโลยีสารสนเทศมากขึ้น ทั้งนี้เพื่อเป็นการสร้างข้อได้เปรียบเชิงแข่งขันที่ยั่งยืนขององค์กร

บริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) ถือได้ว่าเป็นองค์กรที่ต้องพึ่งพาเทคโนโลยี ในเรื่องของการแลกเปลี่ยนข้อมูลข่าวสารทางอินเตอร์เน็ต การค้นหาข้อมูลสารสนเทศ การทำธุรกรรมซื้อขายสินค้า โดยเฉพาะอย่างยิ่งคือการให้บริการข้อมูลลูกค้าทางอินเตอร์เน็ต ที่อาจต้องเผชิญกับปัญหาที่เกิดจากการบุกรุก การเข้าถึงข้อมูล และการโจรกรรมข้อมูล ที่มีแนวโน้มเพิ่มความรุนแรงสูงขึ้น เนื่องจากระบบเครือข่ายมีความเชื่อมโยงถึงกัน ซึ่งความไม่มั่นคงปลอดภัยดังกล่าวก่อให้เกิดความเสียหายและการสูญเสียทรัพยากรสารสนเทศที่หลายองค์กรยากจะหลีกเลี่ยงได้ นอกจากนี้ความเสี่ยงที่มีผลต่อความมั่นคงปลอดภัย ยังอาจเกิดจากระบบการควบคุมภายในด้านระบบสารสนเทศภายในองค์กรที่อาจจะมีประสิทธิผลไม่เพียงพอ และยังรวมไปถึงสาเหตุที่เกิดจากภัยธรรมชาติ การจราจล อุบัติเหตุ เหตุการณ์ร้ายแรงต่าง ๆ ที่ไม่คาดคิดซึ่งปัจจุบันสามารถเกิดขึ้นได้ตลอดเวลา และบางเหตุการณ์ก็อยู่เหนือการควบคุมและการป้องกันขององค์กร

การที่พนักงานละเลยไม่ได้ใส่ใจเรื่องความปลอดภัยข้อมูลอย่างเพียงพอก็เป็นอีกสาเหตุหนึ่งที่มีผลกระทบต่อความไม่ปลอดภัยของข้อมูล ดังนั้นหากผู้บริหารไม่ใส่ใจหรือไม่ให้ความสำคัญ ก็ยิ่งส่งผลกระทบต่อความปลอดภัยของข้อมูลระบบสารสนเทศขององค์กรอย่างหลีกเลี่ยงไม่ได้ ดังนั้นจึงควรให้ความรู้พนักงานทุกคนตั้งแต่ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้ตรวจสอบภายใน รวมถึงผู้ใช้คอมพิวเตอร์ทุกคนในองค์กร เพื่อให้ตระหนักและเข้าใจถึงภัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลภายในองค์กรในปัจจุบัน

แนวคิด ทฤษฎี และการศึกษาวิจัยที่เกี่ยวข้อง

1. กรอบแนวความคิด ทฤษฎี และมาตรฐานที่เกี่ยวข้องกับการรักษาความปลอดภัยสารสนเทศ

ความไม่มั่นคงปลอดภัยเป็นเรื่องที่ไม่สามารถคาดการณ์ได้ล่วงหน้าถึงเหตุการณ์ที่จะเกิดขึ้นในอนาคต และผลกระทบที่ตามมาอาจก่อให้เกิดความเสียหายต่อองค์กรได้ ดังนั้นการบริหารจัดการความมั่นคงปลอดภัยนั้นจึงจำเป็นต้องมีการวางแผนควบคุมความมั่นคงปลอดภัย โดยใช้มาตรฐานที่เกี่ยวข้องดังนี้คือ

1.1 การรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยของข้อมูลข่าวสาร หรือการรักษาความลับนั้น มีมานานตั้งแต่มนุษย์เริ่มมีการติดต่อสื่อสารกัน โดยคาดหวังว่าสิ่งที่ตนเองต้องการเปิดเผยได้ถูกจำกัดอยู่ในขอบเขตที่ตนเองต้องการ สิ่งสำคัญที่จะต้องถูกปกป้องคือ สาระของข่าวสาร ต่อมาการสื่อสารของมนุษย์ได้ถูกพัฒนาไปตามเทคโนโลยีที่ทันสมัย การรักษาความปลอดภัยของข้อมูลข่าวสารจึงต้องขยายวงกว้างออกไปให้ครอบคลุมถึงสื่อกลางที่ใช้นั้นด้วย เช่นการใช้หมึกเขียนชนิดพิเศษที่ต้องใช้เทคนิคบางประการในการทำให้ปรากฏ การใช้หีบหรือกล่องนิรภัย การใช้รหัส การถอดรหัส ตลอดจนถึงการใช้ระบบตรวจสอบ และการกำหนดสิทธิของผู้ใช้ในระบบคอมพิวเตอร์ และระบบอินเตอร์เน็ต ซึ่งเป็นสื่อกลางในการสื่อสารของมนุษย์ในปัจจุบัน

1.2 มาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 27001 (The International Organization for Standardization / The International Electrotechnical Commission 27001)

เป็นมาตรฐานที่เกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ได้รับการพัฒนามาจาก Information Security Management Standard BS7799 ออกโดย British Standard Institute (BSI) ซึ่งมาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization) ที่ถูกกำหนดเพื่อเป็นแนวทางการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยมีการกำหนดแนวทางสำหรับองค์กรในด้านการปฏิบัติงาน การจัดการเพื่อให้เกิดประสิทธิภาพ การพัฒนามาตรฐานความปลอดภัย เพื่อการสร้างความมั่นใจในการเชื่อมโยงระหว่างองค์กร เนื่องจากข้อมูลขององค์กรถือว่าเป็นสินทรัพย์ที่มีความสำคัญ ดังนั้น การรักษาความปลอดภัยของข้อมูล การวิเคราะห์และการบริหารความเสี่ยงที่อาจเกิดขึ้นจึงถือเป็นสิ่งที่สำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ มาตรฐาน ISO/IEC 27001

1.3 มาตรฐานการรักษาความปลอดภัยสารสนเทศ ISO/IEC 17799

มาตรฐานการรักษาความปลอดภัย ISO/IEC 17799 เป็นมาตรฐานด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ (Information Security Management System: ISMS) ที่มีความเกี่ยวข้องกับข้อมูลโดยตรง เนื่องจากการรักษาความปลอดภัยของข้อมูล เป็นส่วนสำคัญส่วนหนึ่งในการบริหารหน่วยงานให้มีประสิทธิภาพ

1.4 การศึกษาแนวทางปฏิบัติตามมาตรฐานมาประยุกต์ใช้งาน สามารถแบ่งออกเป็นส่วน ๆ ได้ดังนี้

1.4.1 มาตรฐานการรักษาความปลอดภัยของข้อมูลในต่างประเทศ

1.4.2 มาตรฐานการรักษาความปลอดภัยของข้อมูลในประเทศไทย

2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3. ข้อมูลที่ใช้ในการวิจัย เป็นการศึกษางานวิจัยในเรื่องที่เกี่ยวข้อง มีรายละเอียดดังนี้คือ

3.1 งานวิจัยเรื่อง การศึกษาแนวทางการพัฒนานโยบายความมั่นคงปลอดภัยในองค์กร ISO27001 กรณีศึกษาบริษัท NEC Corporation (Thailand) Ltd. จำกัด

3.2 งานวิจัยเรื่อง การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสำหรับองค์กรขนาดใหญ่และขนาดกลาง ในเขตกรุงเทพมหานคร

ระเบียบวิธีวิจัย

วิธีการเก็บข้อมูล

ประชากร

ประชากรที่ใช้ในงานศึกษาครั้งนี้คือ พนักงานบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) จำนวนทั้งหมด 120 คน ซึ่งแบ่งเป็น 2 ส่วน คือ

1.1 กลุ่มคณะผู้บริหาร จำนวน 6 คน ประกอบด้วย ผู้บริหาร หัวหน้าฝ่ายปฏิบัติการข้อมูล หัวหน้าฝ่ายระบบคอมพิวเตอร์ หัวหน้าฝ่ายประมวลผลข้อมูล หัวหน้าฝ่ายทรัพยากรบุคคล และหัวหน้าฝ่ายธุรการ

1.2 พนักงานทั้งหมดของบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) จากจำนวนพนักงานทั้งสิ้น 114 คน แบ่งออกเป็น 2 กลุ่มคือ

1.2.1 กลุ่มพนักงานฝ่ายปฏิบัติการข้อมูล ฝ่ายระบบคอมพิวเตอร์ และฝ่ายศูนย์ประมวลผลข้อมูล จำนวน 48 คน ที่เกี่ยวข้องต่อการนำข้อมูลเข้า

ระบบ และการนำระบบการรักษาความปลอดภัยเทคโนโลยีสารสนเทศมาใช้

1.2.2 กลุ่มพนักงานทั่วไปที่เป็นผู้ใช้งานระบบเทคโนโลยีสารสนเทศ จำนวน 66 คน

การวิเคราะห์ข้อมูลและสถิติที่ใช้

การวิเคราะห์ข้อมูลทำโดยการนำข้อมูลที่เก็บรวบรวมได้จากแบบสอบถามทั้งหมดมาทำการวิเคราะห์โดยใช้ ค่าความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และจะนำเสนอข้อมูลที่วิเคราะห์ได้ในลักษณะข้อมูลเชิงสถิติตัวเลข เพื่อประเมินประสิทธิผลของระบบการควบคุมภายในสารสนเทศ เรื่องการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 มีรายละเอียดดังนี้

1. ค่าความถี่ (Frequency) และค่าร้อยละ (Percentage) ใช้สำหรับวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ซึ่งประกอบด้วยเพศ ระยะเวลาที่ทำงานในองค์กรปัจจุบัน ระดับการศึกษา ตำแหน่งงาน และหน่วยงานที่สังกัด

2. ค่าเฉลี่ย (Mean) ใช้สำหรับวิเคราะห์ระดับการประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 ของบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) ตามข้อกำหนด 11 หมวดมาตรฐานของ ISO27001 โดยใช้เกณฑ์การจัดลำดับคะแนนเฉลี่ยดังนี้

ผลการศึกษา

การสรุปค่าเฉลี่ยรวม ในการประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศ ตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 และตามข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ร.บ.2550 ของบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน)

แบบประเมินองค์กรตาม ISO/IEC 27001	ค่าเฉลี่ยรวม	การแปลผล
1. นโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร	3.65	ดี
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร	3.78	ดี
3. การบริหารจัดการทรัพย์สินขององค์กร	3.68	ดี
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร	3.84	ดี
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	3.78	ดี
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร	3.79	ดี
7. การควบคุมการเข้าถึง	4.02	ดี
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบ	3.87	ดี
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร	3.87	ดี
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร	3.96	ดี
11. การปฏิบัติตามข้อกำหนด	4.00	ดี
12. การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 27001	3.90	ดี
13. การปฏิบัติตามข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ร.บ.2550	4.34	ดีมาก

พบว่าประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศ ตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 ของบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) ตามข้อกำหนด 11 หมวดของมาตรฐาน ISO27001 แสดงให้เห็นว่า การควบคุมภายในการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO/IEC 27001 อยู่ในระดับดี รวมถึงการปฏิบัติตามข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ร.บ.2550 และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ อยู่ในระดับดีมาก

ผลการศึกษาสรุปได้ว่า บริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) โดยภาพรวมมีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 ในระดับที่ดี ระดับการประเมินประสิทธิผลระบบการควบคุมภายในด้านสารสนเทศ ตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001 ตามข้อกำหนด 11 หมวดของมาตรฐาน โดยแยกพิจารณาตามข้อกำหนดแต่ละหมวด ดังนี้

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001	หมวดตามมาตรฐาน	คิดเป็นร้อยละ
ระดับดีมาก	หมวดที่ 5 : 5.1.2 หมวดที่ 7 : 7.2.3, 7.3.1, 7.5.3	3.01
ระดับดี	หมวดที่ 1 : 1.1.1, 1.1.2 หมวดที่ 2 : 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.2.1, 2.2.2, 2.2.3 หมวดที่ 3 : 3.1.1, 3.1.2, 3.1.3, 3.2.1, 3.2.2 หมวดที่ 4 : 4.1.1, 4.1.2, 4.1.3, 4.2.1, 4.2.2, 4.2.3, 4.3.1, 4.3.2, 4.3.3 หมวดที่ 5 : 5.1.1, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.2.1, 5.2.2, 5.2.3, 5.2.5, 5.2.6 หมวดที่ 6 : 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.2.1, 6.2.2, 6.2.3, 6.3.1, 6.3.2, 6.4.1, 6.4.2, 6.5.1, 6.6.1, 6.6.2, 6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.8.1, 6.8.2, 6.8.3, 6.8.4, 6.8.5, 6.9.1, 6.9.2, 6.9.3, 6.10.1, 6.10.2, 6.10.3, 6.10.4	94.74

การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO27001	หมวดตามมาตรฐาน	คิดเป็นร้อยละ
	หมวดที่ 7 : 7.1.1, 7.2.1, 7.2.2, 7.2.4, 7.3.2, 7.3.3, 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.7, 7.5.1, 7.5.2, 7.5.4, 7.5.5, 7.5.6, 7.6.1, 7.6.2, 7.7.1, 7.7.2 หมวดที่ 8 : 8.1.1, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.3.1, 8.3.2, 8.4.1, 8.4.2, 8.4.3, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.6.1 หมวดที่ 9 : 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3 หมวดที่ 10 : 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5 หมวดที่ 11 : 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.2.1, 11.2.2, 11.3.1, 11.3.2	
ระดับดีพอใช้	หมวดที่ 5 : 5.2.4 หมวดที่ 6 : 6.10.5, 6.10.6	2.25

ข้อเสนอแนะ

จากผลการสำรวจการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยของข้อมูล ISO2701 ของบริษัท บิซิเนสออนไลน์ จำกัด (มหาชน) พบว่าระบบการควบคุมภายในด้านสารสนเทศ อยู่ในระดับที่ดี มีเพียง 3 เรื่องที่มีการปฏิบัติตามมาตรฐานที่ดีพอใช้ แต่ยังมีข้อบกพร่องอยู่บ้างคือ

ข้อกำหนดที่ 5.2.4 การบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพสมบูรณ์

ข้อกำหนดที่ 6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด

ข้อกำหนดที่ 6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน

ดังนั้นหากบริษัทต้องการมีการควบคุมภายในเรื่องดังกล่าวในระดับมากถึงมากที่สุด บริษัทต้องให้ความสนใจในเรื่องที่ยังไม่ได้มีการปฏิบัติตามมาตรฐานในระดับที่เพียงพอ ดังนี้คือ

1. ข้อกำหนดที่ 5.2.4

การบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพสมบูรณ์

บริษัทควรเพิ่มมาตรการเพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก โดยควรเพิ่มมาตรการการบำรุงรักษาอุปกรณ์ 2 เรื่องคือ

1.1 กระบวนการควบคุมและการเก็บรักษาอุปกรณ์

1.1.1 กำกับดูแลเจ้าหน้าที่ให้มีการปฏิบัติงานเป็นไปตามกฎหมาย ระเบียบและวิธีการใช้อุปกรณ์อย่างเคร่งครัด

1.1.2 ปรับปรุงแนวปฏิบัติหรือคู่มือเกี่ยวกับการใช้อุปกรณ์แต่ละประเภทตามความเหมาะสมและกรณีที่เป็นอุปกรณ์ที่มีเทคโนโลยีที่ซับซ้อนควรจัดให้มีการอบรมในการใช้อุปกรณ์เหล่านั้นด้วย

1.1.3 จัดกิจกรรมเสริมสร้างจิตสำนึกที่ดีแก่เจ้าหน้าที่รวมทั้งการใช้ ดูแลรักษา อุปกรณ์ของบริษัทให้สมประโยชน์

1.1.4 สอบทานการจัดทำทะเบียนคุมอุปกรณ์ให้เป็นปัจจุบัน

1.1.5 จัดให้มีระบบการรายงานการใช้อุปกรณ์ประจำปี

1.2 กระบวนการซ่อมแซมและการบำรุงรักษาอุปกรณ์

1.2.1 กำหนดแผนการซ่อมบำรุงรักษาประจำปีของอุปกรณ์ประเภทต่างๆ ให้ชัดเจน

1.2.2 กำหนดหรือมอบหมายการดูแลรักษาอุปกรณ์ให้อยู่ในความรับผิดชอบของผู้ที่ใช้อุปกรณ์ที่มีมูลค่า หรือจำเป็นต้องมีการดูแลรักษาเป็นพิเศษ

1.2.3 จัดให้มีการตรวจสอบหรือสอบทานอุปกรณ์อย่างสม่ำเสมอ

1.2.4 จัดทำทะเบียนประวัติและการซ่อมบำรุงรักษาอุปกรณ์ให้เป็นปัจจุบัน และตรวจสอบทะเบียนการซ่อมบำรุงกับรายงานการซ่อมบำรุงของหน่วยงานนั้น

2. ข้อกำหนดที่ 6.10.5

การบันทึกเหตุการณ์ข้อผิดพลาด

บริษัทควรกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร โดยปัจจุบันบริษัทมีการดำเนินการในเรื่องดังกล่าวแล้ว แต่ยังขาดในส่วนรวบรวมรายงานเหตุการณ์ที่เกิดขึ้นจาก Incident Event Report Form เพื่อจัดทำรายงานประจำสัปดาห์ เสนอให้ต่อผู้บริหารทราบ

3. ข้อกำหนดที่ 6.10.6

การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน

ผู้ดูแลระบบต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

วิธีการตั้งเวลาให้ตรงตาม กรมอุทกศาสตร์ กองทัพเรือ

1. คลิกขวาที่เวลา ที่มุมขวาล่างของหน้าจอ Windows
2. คลิกหัวข้อ Adjust Date/Time
3. ที่แท็ป Internet Time
4. ให้คลิกเครื่องหมายถูก หน้าข้อความ "Automatically synchronize with an internet time server" และ
5. พิมพ์ข้อความนี้ในช่อง "server" ว่า time.navy.mi.th
6. คลิกปุ่ม Update Now
7. คลิกปุ่ม Apply และตามด้วย OK เพื่อยืนยัน