



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ของบริษัท เซ็น คอร์ปอเรชั่น กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย

(Information Technology Security Policy)

Version 6.0.0

คำนำ

การดำเนินกิจการปัจจุบัน ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับบริษัทเซ็น คอร์ปอเรชั่น กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย (บริษัท อากะ อินเตอร์ พู๊ดส์ จำกัด, บริษัท โตเกียว คอนเซปต์ จำกัด, บริษัท เซ็น แอนด์ สไปซี่ จำกัด, บริษัท กิวกริลกรุ๊ป จำกัด, บริษัท เซ็นเรสเตอร์รองโฮลดิ้ง จำกัด และบริษัท เซ็น ซัพพลาย เซน แมเนจเม้นท์ จำกัด) ที่เข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของบริษัทฯ และบริษัทย่อย แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่างๆ แต่ในขณะเดียวกันก็มีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติงานได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่างๆ ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายทั้งภายในและภายนอก เพื่อก่อวินโหรบบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับของบริษัทฯ และบริษัทย่อย ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก และทำให้สูญเสียชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้นผู้ให้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัย ด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น บริษัทฯ จึงจัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ("นโยบายฯ") เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตาม การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายฯ จากทุกหน่วยงานและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว บริษัทฯ จึงหวังเป็นอย่างยิ่งว่านโยบายฯ ฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทฯและบริษัทย่อยทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

สารบัญ

	หน้า
ส่วนที่ 1 ความหมายและคำจำกัดความ	5
ส่วนที่ 2 นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	
หมวดที่ 1 นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)	11
หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Technology Security)	11
หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)	13
หมวดที่ 4 การบริหารจัดการและควบคุมทรัพย์สิน (Asset Management)	14
หมวดที่ 5 การควบคุมการเข้าถึง (Access Control Policy)	18
หมวดที่ 6 การจัดการชั้นความลับของสารสนเทศ (Information Classification Policy)	23
หมวดที่ 7 การเข้ารหัสข้อมูล (Cryptography)	24
หมวดที่ 8 ความมั่นคงทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)	25
หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)	27
หมวดที่ 10 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)	31
หมวดที่ 11 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development, and maintenance)	32
หมวดที่ 12 การบริหารงานและความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)	35
หมวดที่ 13 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Information Technology Security Incident Management)	36
หมวดที่ 14 การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร (Information Technology Security aspects of business continuity management)	32
หมวดที่ 15 ความสอดคล้อง (Compliance)	38
หมวดที่ 16 การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security Management)	40



ส่วนที่ 3 ข้อกำหนดและแนวปฏิบัติความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (Procedure and guideline)

แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย	42
แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ	44
แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย	46
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	47
แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน	48
แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ	50
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ	51
แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ	53
แนวปฏิบัติการสำรองและการกู้คืนข้อมูล	54
แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ	58
แนวปฏิบัติในการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล	60
แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	61
แนวปฏิบัติการควบคุมการเข้าถึงจากทางไกล (Remote Access)	65
ข้อกำหนดการใช้งานเครือข่าย	67
แนวปฏิบัติในการพัฒนาระบบ	68
แนวปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)	71
ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)	71
แนวปฏิบัติการสร้างความตระหนักเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ	74

ส่วนที่ 1

ความหมายและคำจำกัดความ

1. บริษัทฯ หมายถึง บริษัท เซ็น คอร์ปอเรชั่น กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย (บริษัท อากะ อินเตอร์ ฟู้ดส์ จำกัด, บริษัท โตเกียว คอนเซ็ปท์ จำกัด, บริษัท เซ็น แอนด์ สไปซี่ จำกัด, บริษัท กิวกกริลกรุ๊ป จำกัด, บริษัท เซ็นเรสเตอร์รองโฮลดิ้ง จำกัด และบริษัท เซ็น ชัฟฟลาย เซน แมเนจเม้นท์ จำกัด)
2. คณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Support Team: ITST) คณะทำงานด้านไอทีที่ประกอบด้วยหัวหน้ากลุ่มเทคโนโลยี และทีมงานทั้งด้านโครงสร้างพื้นฐาน (Information Infrastructure) ทีมงานด้านช่วยเหลือแนวทางแก้ปัญหาด้านโปรแกรม (Software Solutions) และ ทีมงานพัฒนาโปรแกรม (Application) ทำหน้าที่ กำหนดโครงสร้างความปลอดภัยสารสนเทศ ทบทวน ปรับปรุงนโยบาย (policy) แนวปฏิบัติ (procedure) และ Guide line นำเสนอให้ประธานเจ้าหน้าที่บริหารพิจารณาอนุมัติ และควบคุมการปฏิบัติงานโดยตรง
3. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของบริษัทฯ และบริษัทย่อย โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งบริษัทฯ กำหนดไว้
4. หน่วยงานภายนอก หมายถึง บริษัทใดๆ หรือ Franchisee หรือหน่วยงานภายนอกที่บริษัทฯ และบริษัทย่อยอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆของหน่วยงานของบริษัทฯ และบริษัทย่อย โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
5. ฝ่าย IT (Information Technology)/ฝ่ายเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ดูแล และให้บริการ ด้านเทคโนโลยีและสารสนเทศของบริษัท เซ็น คอร์ปอเรชั่น กรุ๊ป (มหาชน) และบริษัทย่อย
6. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง รูปภาพ หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
7. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ
8. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

9. ระบบเครือข่าย (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆของบริษัทฯได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต เป็นต้น
10. ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อบรรยากาศคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน ในระยะใกล้ เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
11. ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อบรรยากาศคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
12. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
13. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
14. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก
15. ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
16. จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
17. ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
18. ผู้บริหารระดับสูงสุด หมายถึง ประธานเจ้าหน้าที่บริหาร หรือกรรมการบริหาร

19. เจ้าหน้าที่ด้านไอที หมายถึง ผู้ที่ได้รับมอบหมายให้กำกับดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของบริษัทฯ
20. ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
21. ผู้ดูแลระบบ (System administrator) หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บริหารด้านไอที ให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ให้บริการได้อย่างมีประสิทธิภาพ
22. ผู้พัฒนาระบบ (Developer) หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ
23. เจ้าหน้าที่ หมายความว่า บุคลากรที่สังกัดหน่วยงานต่างๆ ของบริษัท
24. ผู้ใช้งาน (user) บุคคลที่มีบัญชีรายชื่อที่ออกโดยฝ่ายเทคโนโลยีและ/หรือหน่วยงานที่ได้รับอนุญาตเช่นฝ่าย HR ให้ใช้ระบบสารสนเทศของบริษัทฯ
25. การรักษาความมั่นคงปลอดภัยฯ หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ และการสื่อสาร
26. มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
27. วิธีการปฏิบัติ (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
28. แนวปฏิบัติ (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
29. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ
30. เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
31. ทรัพย์สิน หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์เครือข่าย เลขที่อยู่ไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน
32. ห้องควบคุมระบบ หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของบริษัทฯ ภายใต้การดูแลของ ฝ่ายเทคโนโลยี
33. สื่อบันทึกพกพา (portable media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD , flash drive, External hard disk ฯลฯ
34. ชื่อผู้ใช้ (username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งาน

- ระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้
35. รหัสผ่าน (password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตนบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ
36. การเข้ารหัสลับ (encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีรหัส และโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
37. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน และหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ
38. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัย
39. การพิสูจน์ยืนยันตัวตน (authentication) หมายความว่า ขั้นตอนการรักษาความมั่นคงปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้บริการระบบ ทัวไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
40. MAC Address (media access control address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างอิงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
41. WEP (wired equivalent privacy) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
42. WPA (Wi-Fi protected access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
43. VPN (virtual private network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
44. แผนผังระบบเครือข่าย (network diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของบริษัทฯ

W. Thanthy

45. SOC (Security Operation Center) คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบ และแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง
46. ระบบคลาวด์ (Cloud) ย่อมาจาก "Cloud Computing" แต่จะแรกสั้นๆ ว่า Cloud คือ เครื่องมือหรือ การบริการ System Host (ระบบที่เป็นตัวกลางไว้ควบคุม System อื่นๆ) ต่างๆ ผ่าน อินเทอร์เน็ต
47. VA ((Vulnerability Assessment) คือช่องโหว่ หรือช่องทางที่ไม่พึงประสงค์ของการเข้ามาทำลายระบบเทคโนโลยีสารสนเทศ ผ่านช่องทางเครือข่าย Network
48. Pen Test (Penetration Test) คือ การทดสอบเจาะโปรแกรมระบบเชิงลึก ซึ่งจะใช้ในการตรวจสอบโปรแกรม โดยละเอียด
49. Monitoring Tool ระบบการตรวจจับความผิดปกติ โดยแยกออกเป็นแต่ละส่วน เช่น ส่วนงานการเชื่อมต่อระบบเครือข่าย หรือ ส่วนงานโปรแกรม เป็นต้น
50. SSL – Socket Secure Level เป็นระบบรักษาความปลอดภัยทางด้านอินเทอร์เน็ต โดยจะมีการติดตั้งที่ระบบเว็บไซต์ของบริษัทฯ ทุกเว็บไซต์
51. การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกของบริษัท อันกระทบต่อการดำเนินกิจการ
52. ภัยคุกคามทางไซเบอร์ (Cyber Threat) การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมีมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
53. ไซเบอร์ (Cyber) ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
54. เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident) เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

w.Thanthis

55. หน่วยงานควบคุมหรือกำกับดูแล (Regulator) หน่วยงาน หรือ บุคคลซึ่งมีการแต่งตั้ง กำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของบริษัทหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
56. แพลตฟอร์ม (Platform) ระบบโปรแกรมคอมพิวเตอร์ที่สามารถขยายขีดความสามารถอย่างไม่จำกัด มีการพัฒนาฟังก์ชันหรือโมดูลใหม่ๆ มาต่อยอดอยู่ตลอดเวลา เกิดนวัตกรรมใหม่ๆ เสมอ และสามารถนำไปต่อเชื่อมกับระบบอื่นได้ แพลตฟอร์มไม่ได้จำกัดอยู่แค่ซอฟต์แวร์แต่ยังรวมไปถึงเว็บไซต์ หรือบริการที่คนอื่นสามารถเขียนโปรแกรมมาต่อเชื่อมหรือดึงข้อมูลได้โดยอัตโนมัติ
57. ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ศาสตร์แขนงหนึ่งของวิทยาศาสตร์คอมพิวเตอร์ ที่เกี่ยวข้องกับวิธีการทำให้คอมพิวเตอร์มีความสามารถคล้ายมนุษย์หรือเลียนแบบพฤติกรรมมนุษย์ โดยเฉพาะความสามารถในการคิดเองได้ หรือมีปัญญา ซึ่งปัญญานี้มนุษย์เป็นผู้สร้างให้คอมพิวเตอร์ จึงเรียกว่าปัญญาประดิษฐ์ มุมมองต่อ AI ที่แต่ละคนมีอาจไม่เหมือนกัน ขึ้นอยู่กับว่าเราต้องการความฉลาดด้อยค่าไปถึงพฤติกรรมที่มีต่อสิ่งแวดล้อมหรือคำนึงการคิดได้ของผลผลิต AI
58. ทีมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer emergency response team: CERT) CERT หรือ Computer Emergency Response Team เป็นเครื่องหมายการค้าจดทะเบียนของ CERT Coordination Center (CERT/CC) หมายถึงหน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute – SEI) ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่ และต้องการใช้ชื่อ เช่น ประเทศไทย มี Thai CERT
59. แพตช์ (Patch) โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
60. Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ
61. Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
62. Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของบริษัท และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

ส่วนที่ 2

หมวดที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy)

วัตถุประสงค์ เพื่อกำหนดทิศทางและสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยให้สอดคล้องกับภารกิจขององค์กร และไม่ขัดต่อกฎหมาย ศีลธรรมอันดี ระเบียบ ประกาศและ ข้อบังคับที่เกี่ยวข้อง

นโยบาย

1.1 เอกสารนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy Document)

1.1.1 คณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรเพื่อให้เกิดความมั่นใจและมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายสื่อสารข้อมูล โดยนโยบายฯ ได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหารเพื่อนำไปปฏิบัติงาน

1.1.2 คณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีการเผยแพร่ เอกสารนโยบายฯ ให้กับผู้ใช้งาน หน่วยงานภายใน และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

1.1.3 การทบทวนการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ คณะทำงานจะดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายฯ ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

1.1.4 การตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในเอง หรือผู้ตรวจสอบภายนอก ทั้งนี้เป็นไปตามนโยบายของบริษัทฯ

1.1.5 กรณีที่มีเหตุการณ์ หรือพบสิ่งกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ จะต้องทำการแจ้งให้หน่วยงานเทคโนโลยีโดยเร็ว หรือแจ้งขั้นตอนการปฏิบัติที่กำหนด

1.1.6 รายละเอียด หรือวิธีปฏิบัติที่เกี่ยวข้องจะมีขั้นตอนที่แยกออกจากนโยบายฉบับนี้ เพื่อความปลอดภัยในการดำเนินงาน

หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of Information Technology Security)

2.1 โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศภายในองค์กร (Internal organization)

2.1.1 การกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security roles and responsibilities) ประธานเจ้าหน้าที่บริหารเป็นผู้แต่งตั้งกลุ่มหรือคณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

1) หัวหน้ากลุ่มเทคโนโลยี กำหนดตำแหน่งงานและทีมงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กำหนดความรับผิดชอบให้เหมาะสม พร้อมทั้งควบคุมการปฏิบัติงานเพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

2) หัวหน้ากลุ่มเทคโนโลยี เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และ ทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

3) ผู้บริหารทุกหน่วยงานของบริษัทฯและบริษัทย่อย มีหน้าที่รับผิดชอบ ให้ความร่วมมือดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

4) ผู้ใช้งาน และหน่วยงานภายนอก เช่น Franchisee หรือคู่ค้า ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัทฯในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

5) ระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่ฝ่ายเทคโนโลยี ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้ากลุ่มเทคโนโลยี มีหน้าที่

- ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนหรือภัยพิบัติ
- รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย และการควบคุมการเข้าใช้งานคลาวด์ (Cloud) ในระดับผู้ดูแล
- ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด
- ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต
- ตรวจสอบ และประสานงานกับผู้ให้บริการด้านความปลอดภัยที่มีการแต่งตั้งหรือว่าจ้าง
- ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ

2.1.3 การติดต่อกับหน่วยงานภายนอก (Contact with authorities)

1) มีการจัดทำรายชื่อ และข้อมูลสำหรับติดต่อกับหน่วยงาน และ suppliers เช่น

- ผู้ให้บริการด้านอินเทอร์เน็ต (Internet provider)
- การไฟฟ้านครหลวง



- สำนักงานตำรวจแห่งชาติ
- ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT)
- ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
- หน่วยงานควบคุม หรือกำกับดูแลภายในองค์กร (Regulator)

เพื่อใช้สำหรับติดต่อประสานงานด้านความมั่นคงปลอดภัย เพื่อควบคุมกิจการให้ดำเนินงานได้ถูกต้อง

หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

3.1 การสรรหาบุคลากรก่อนการทำงาน (Prior to employment) เพื่อคัดสรรพนักงานที่ตรงกับความต้องการ และเพื่อให้พนักงานเข้าใจในหน้าที่และความรับผิดชอบ

นโยบาย

3.1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

- มีการตรวจสอบคุณสมบัติที่เกี่ยวข้องกับการปฏิบัติงาน เช่น ประวัติการศึกษา ประวัติการทำงานของบริษัทที่ผ่านมา
- มีการทดสอบคุณสมบัติที่ใช้ในการปฏิบัติงานเบื้องต้น

3.2.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

1) มีการกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับหน่วยงานภายนอกที่จ้างมาปฏิบัติงาน และสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

2) ลงนามในสัญญาระหว่างพนักงานและหน่วยงานว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement : NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้นๆ ทั้งนี้จะมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี หลังจากสิ้นสุดการว่าจ้างแล้ว

3) เพื่อให้การบริหารจัดการบัญชีผู้ใช้ เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด เจ้าหน้าที่บุคคลที่ดูแลทรัพยากรบุคคลส่วนกลางของบริษัทฯ จะแจ้งให้ฝ่ายเทคโนโลยี ทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากการงาน หรือการสิ้นสุดการเป็นผู้บริหาร พนักงาน และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

3.2 ระหว่างการจ้างงาน (During employment) เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของตนเอง

3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

1) ผู้ใช้งาน และหน่วยงานภายนอกที่จ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

3.2.2 สร้างความตระหนัก ให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security awareness, education and training)

- 1) เจ้าหน้าที่ใหม่ได้รับการอบรมเกี่ยวกับเรื่องนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเบื้องต้น โดยเป็นส่วนหนึ่งของการปฐมนิเทศพนักงาน
- 2) เจ้าหน้าที่ทุกคน จะมีการอบรมเกี่ยวกับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ เช่น หลักสูตรความรู้พื้นฐานด้านเทคโนโลยี การตระหนักความปลอดภัยด้านไซเบอร์ หรือหลักสูตรด้านความคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นต้น อย่างน้อยปีละ 1 ครั้ง
- 3) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ จะได้รับการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศเชิงลึก และเป็นหลักสูตรที่เป็นของฝ่ายที่ดูแลโดยเฉพาะ อย่างน้อยปีละ 1 ครั้ง

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment) เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ในกรณียกเลิกหรือเปลี่ยนแปลงสิทธิกับเจ้าหน้าที่ หรือเปลี่ยนแปลงการจ้างงาน

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)

- 1) หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ จะถูกยกเลิกสิทธิการเข้าถึงข้อมูลในระบบสารสนเทศ
- 2) หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน จะถูกยกเลิกการมีเป็นสมาชิกส่วนลดของพนักงาน

หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset Management)

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) ส่วนการป้องกันความเสียหายจากปัจจัยสถานะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่างๆ ที่บริษัทฯ จัดให้มี

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets) เพื่อให้ระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนทรัพย์สิน จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

4.1.1 บัญชีทรัพย์สินที่ภายใต้การดูแลของฝ่ายเทคโนโลยี (Inventory of assets)

1) มีการจัดทำและเก็บทะเบียนทรัพย์สินเทคโนโลยีเพื่อเป็นข้อมูลสำหรับนำไปใช้ติดตามตรวจสอบในระบบ โดยมีการจัดเก็บข้อมูลเป็นหมวดหมู่ แยกออกเป็นกลุ่มดังนี้

- a) ทรัพย์สินประเภทฮาร์ดแวร์ และอุปกรณ์สำนักงาน เครื่องแม่ข่าย อุปกรณ์เครือข่าย
- b) ทรัพย์สินประเภทซอฟต์แวร์
- c) ทรัพย์สินประเภทข้อมูล
- d) ระบบ Cloud

และมีการลงทะเบียนรายละเอียดทรัพย์สิน อย่างน้อยต้องมี รหัสทรัพย์สิน (Asset Number) ผู้ถือครองทรัพย์สิน หมายเลขรหัสประจำทรัพย์สิน (Serial Number) และตำแหน่งที่จัดเก็บ หรือหน่วยงาน

2) มีการตรวจสอบทรัพย์สินตามระยะเวลาที่กำหนด เช่น ปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยอาจจะเป็นการดำเนินการของฝ่ายหรือหน่วยงานที่บริษัทแต่งตั้งขึ้น

3) อุปกรณ์เครื่องคอมพิวเตอร์ส่วนตัว ที่มีการใช้งานอย่างน้อย 4 ปี จากวันที่มีการซื้อเข้ามาใช้งาน ฝ่ายเทคโนโลยีสารสนเทศจะมีตรวจสอบ เพื่อประเมินสภาพการใช้งาน และเสนอพิจารณาการปรับเปลี่ยนเครื่อง ที่ได้รับการอนุมัติจากหัวหน้างาน ตามเกณฑ์คุณลักษณะของแต่ละหน้าที่ และเครื่องที่ถูกเปลี่ยนจะสามารถขายให้กับผู้ใช้งานเดิมได้ ในราคาขอมเยา หรือราคาที่ได้มีการอนุมัติตามนโยบาย

4) มีการจัดความสำคัญของประเภททรัพย์สินตามประเภทความสำคัญ เช่น เครื่องแม่ข่ายมีความสำคัญมาก และเครื่องลูกข่าย มีความสำคัญรองลงไป เป็นต้น

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of assets)

- 1) มีการกำหนดผู้รับผิดชอบทรัพย์สินในทะเบียนทรัพย์สินในระบบสารสนเทศที่ชัดเจน
- 2) ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมทรัพย์สิน ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน
- 3) กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบต่อทรัพย์สินของหน่วยงานที่ได้รับมอบหมาย
- 4) ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

- 5) ผู้ใช้งานมีสิทธิใช้ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์กร
- 6) ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ 5) ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
- 7) ไม่อนุญาตให้พนักงานใช้คอมพิวเตอร์ส่วนตัว ที่ไม่ใช่ของบริษัทจัดหาให้ในการดำเนินงาน โดยไม่ได้รับอนุมัติจากหัวหน้างาน และกรณีพนักงานนำคอมพิวเตอร์ส่วนตัวมาใช้นั้น ข้อมูลทุกอย่างในเครื่องถือว่าเป็นสมบัติของบริษัท

4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของตนเองได้อย่างเหมาะสม ไม่ทำความเสียหาย หรือนำข้อมูลเผยแพร่ให้กับบุคคลภายนอกที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือยืมใช้งานอุปกรณ์สารสนเทศ เช่น คอมพิวเตอร์ ชุดอุปกรณ์ต่อพ่วง(เมาส์, คีย์บอร์ด) หรือระบบงานที่สามารถเข้าถึง เช่น โปรแกรมการขายหน้าร้าน

ในวันที่จะเริ่มปฏิบัติงาน ระหว่างการปฏิบัติงาน จนถึงสิ้นสุดการปฏิบัติงาน จะมีระเบียบการปฏิบัติดังนี้

1) เมื่อเริ่มต้นปฏิบัติงาน การครอบครองอุปกรณ์เทคโนโลยีสารสนเทศ สำหรับพนักงานบริษัทฯ และบริษัทย่อยที่มีสิทธิใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ จะรับอุปกรณ์ได้ที่ฝ่ายบริหารข้อมูลเทคโนโลยีสารสนเทศ โดยอุปกรณ์จะอยู่ในสภาพที่พร้อมใช้งาน อุปกรณ์พื้นฐานจะมีดังนี้

1.1 คอมพิวเตอร์ส่วนตัว จะเป็นแบบตั้งโต๊ะหรือแบบพกพา ขึ้นกับความสะดวกและเหมาะสมกับการปฏิบัติงาน หรือตามคำร้องขอและอนุมัติของหัวหน้าแต่ละสายงานนั้น

1.2 อุปกรณ์ต่อพ่วงพื้นฐาน ได้แก่ เมาส์ คีย์บอร์ด

1.3 โปรแกรมพื้นฐานที่ติดตั้งและปรับค่าการปฏิบัติงานที่เรียบร้อยแล้ว คือ ระบบปฏิบัติการวินโดวส์ (Windows) โปรแกรม Microsoft Office คือ Word, Excel, Power Point, Outlook สำหรับการใช้งานการรับ/ส่ง Email, โปรแกรมสำหรับการเชื่อมต่อเพื่อช่วยเหลือ (Remote Support)

1.4 Email พนักงาน หรือหน่วยงานในสังกัดในบริษัทฯ และบริษัทย่อยที่ใช้ร่วมกัน (Group Email) หรือ Store Email สำหรับสาขา

1.5 โปรแกรมที่ใช้เฉพาะของแต่ละหน่วยงาน คือ

- a) โปรแกรม Navision สำหรับฝ่ายบัญชี ฝ่ายการเงิน ฝ่ายจัดซื้อ ฝ่ายคลังสินค้า
- b) โปรแกรม AutoCAD สำหรับฝ่ายบริหารโครงการ (เฉพาะพนักงานที่ได้รับหน้าที่)

- c) โปรแกรม Adobe Photoshop หรือโปรแกรมการจัดการรูปภาพ สำหรับห้ฝ่ายการตลาด (Marketing) ที่ได้รับมอบหมายเท่านั้น
- d) โปรแกรม HR-Focus สำหรับฝ่ายบริหารบุคคล ตามการดูแลระบบ
- e) โปรแกรม Acrobat เฉพาะหน่วยงานที่มีการร้องขอ และอนุมัติจากหัวหน้าหน่วย

1.6 โปรแกรมป้องกันไวรัส (Anti-Virus)

1.7 ข้อมูลผู้ใช้งานของแต่ละระบบงาน และระบบงานเว็บ (Web Application)

2) ระหว่างการจ้างงาน พนักงานจะต้องดำเนินการที่เหมาะสม ไม่ทำให้อุปกรณ์ชำรุดเสียหาย หรือในการใช้งานระบบ จะไม่ให้เกิดความเสียหายหรือสูญเสียให้เกิดความเสียหาย

3) การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

เพื่อป้องกันผลประโยชน์ของบริษัทฯ และบริษัทย่อย เมื่อมีการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงาน พนักงานหรือผู้ที่ทำสัญญาจ้างต้องนำทรัพย์สินของบริษัทฯ ทั้งหมดที่ตนเองถือครองมาตรวจสอบและนัดหมายการส่งมอบคืนก่อนสิ้นสุดการจ้างงานอย่างน้อย 15 วันทำการ เพื่อเจ้าหน้าที่บริหารข้อมูลสารสนเทศจะได้ทำการตรวจสอบสภาพอุปกรณ์ โดยจะต้องอยู่ในสภาพที่ใช้งานได้ปกติ และนำมาคืนในวันนัดหมาย

ในกรณีที่อุปกรณ์เสียหาย ฝ่ายบริหารข้อมูลเทคโนโลยีสารสนเทศ จะประเมินความเสียหายกับพนักงาน ในราคาที่ตัดเทียบกับผู้ให้บริการ เพื่อชดใช้ค่าเสียหายตามข้อตกลงร่วมกัน

เนื่องด้วยบริษัทไม่มีนโยบายให้พนักงานใช้คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน พนักงานต้องใช้คอมพิวเตอร์ที่บริษัทจัดหาให้เท่านั้น แต่กรณีที่พนักงานใช้เครื่องตัวเองแล้วก่อนนโยบายฉบับนี้ ข้อมูลในเครื่องจะถือว่าเป็นทรัพย์สินของบริษัท

4.1.4 การคืนทรัพย์สิน (Return of assets)

1) พนักงานที่สิ้นสุดการจ้างงาน หรือสิ้นสุดโครงการต้องคืนทรัพย์สินสารสนเทศที่รับผิดชอบทั้งหมดรวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้าออก คอมพิวเตอร์ รวมทั้งข้อมูลภายในเครื่อง และอุปกรณ์ต่อพ่วง คู่มือและอุปกรณ์ต่างๆ

4.1.5 การนำอุปกรณ์สารสนเทศส่วนตัวมาใช้งาน ** บริษัทไม่มีนโยบายให้พนักงานใช้คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน ยกเว้นกรณีที่มีการอนุมัติจากผู้บริหารตั้งแต่ผู้อำนวยการขึ้นไปของแต่ละหน่วยงาน

1) พนักงานจะต้องแจ้งให้ฝ่ายเทคโนโลยีทราบและตรวจสอบก่อนลงทะเบียนเป็นลายลักษณ์อักษร และได้รับอนุมัติจากผู้บริหารสูงสุดของฝ่ายนั้นๆ และ/หรือหัวหน้ากลุ่มเทคโนโลยี

2) อุปกรณ์ดังกล่าวจะต้องใช้ Software ที่ถูกต้องมีลิขสิทธิ์เท่านั้น และมีการติดตั้ง Antivirus อย่างถูกต้อง มีการ Update Security และ Soft patch ที่เป็นปัจจุบันตามรอบที่กำหนด โดยฝ่ายเทคโนโลยี เป็นแบบอัตโนมัติ

3) อุปกรณ์ดังกล่าวจะต้องใช้ IP และ เชื่อมต่อ network ตามที่ฝ่ายเทคโนโลยีกำหนดเท่านั้น

4) กรณีที่พนักงานพ้นสภาพ ข้อมูลในเครื่องส่วนตัวถือว่าเป็นสิทธิ์ของบริษัทฯ ทั้งหมด

4.2 การจัดการสื่อบันทึกข้อมูล (Media Handling) เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต จากการเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูลสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูลโดย

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Removable media)

1) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น Tablet, PDA, Thumb-Drive, CD -Rom เป็นต้น) ที่มีข้อมูลลับขององค์กรบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

2) สื่อบันทึกในรูปแบบคลาวด์ จะสามารถใช้งานได้ตามความสามารถของบัญชีนั้นๆ โดยจะสามารถส่งต่อให้กับบุคคลอื่น ทั้งใน และนอกองค์กรได้ และต้องดำเนินการด้วยความระมัดระวัง เรื่องของการเผยแพร่ข้อมูล

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

1) ข้อมูลลับขององค์กรที่สำเนาเก็บอยู่บนสื่อบันทึกข้อมูล หากไม่ใช้งานแล้วต้องทำลายให้สิ้นซากตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)

1) หากต้องขนย้ายสื่อบันทึกข้อมูลจะต้องป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การล็อกกุญแจ การปิดผนึก หรือการเข้ารหัส เป็นต้น

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

5.1 นโยบายควบคุมการเข้าถึง (Access control policy)

5.1.1 การควบคุมการเข้าถึงเป็นแนวทางปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกเพื่อควบคุมให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และมีการอนุมัติจากหัวหน้างาน โดยมีมาตรการควบคุมการเข้าถึง ให้ปฏิบัติตามแนวปฏิบัติดังต่อไปนี้

- 1) แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ
- 2) แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่ายไร้สาย
- 3) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
- 4) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
- 5) แนวปฏิบัติในการควบคุมการเข้าถึงจากทางไกล

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เป็นนโยบายเพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้โดย

5.2.1 กำหนดให้มีการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and de-registration) การลงทะเบียนผู้ใช้งานใหม่ กำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการเพื่อให้สามารถใช้งาน

ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ ในกรณีที่ผู้ใช้งานสิ้นสุดสถานภาพ ข้อมูลสิทธิจะถูกยกเลิก ออกจากระบบทันทีตาม แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access Provisioning)

ผู้ดูแลระบบมีกระบวนการกำหนดสิทธิให้ครอบคลุมผู้ใช้งานให้ครบทุกประเภทและทุกบริการ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น

บุคคลภายนอกที่ต้องการสิทธิในการใช้งานระบบสารสนเทศของหน่วยงานให้ทางหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right)

ผู้ดูแลระบบมีการกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่รับผิดชอบ โดยให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

ทั้งนี้ การเข้าถึงการสิทธิของระบบการขาย (Point of Sale – POS) จะมีการกำหนดสิทธิการเข้าถึง และการจัดการแยกออกไปตามแต่ละประเภท เนื่องจากข้อจำกัดของระบบที่ไม่เหมือนกัน ซึ่งจะอ้างอิงการจัดการในเอกสารการปฏิบัติงาน (Work Instruction – WI) หรือระเบียบวิธีปฏิบัติงานแยกออกไป

กำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอโดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- บ้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

2) กำหนดเกณฑ์การระดับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

3) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้

- (3.1) อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- (3.2) กำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิการเข้าถึงนั้นอย่างน้อยปีละ 1 ครั้ง

(3.3) ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการ ละเมิด ความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงาน

5.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ผู้ดูแลระบบจะมีการทบทวนสิทธิในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละครั้ง หรือเมื่อมีเหตุที่ต้องดำเนินการ

5.2.5 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights) เมื่อเจ้าหน้าที่ลาออก เปลี่ยนแปลงข้อตกลงหรือหรือสัญญา ผู้ดูแลระบบจะทำการถอดถอน หรือปรับปรุงสิทธิให้ถูกต้องทันทีที่ได้รับแจ้งและอนุมัติจากหน่วยงาน

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน ให้ปฏิบัติตามนโยบายต่อไปนี้

5.3.1 การใช้ข้อมูลลับในการพิสูจน์ตัวตน (Use of secret authentication information)

1) ผู้ใช้งานปฏิบัติตามการควบคุมการเข้าถึงสารสนเทศองค์กร การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านตามแนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

2) รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย

3) ผู้ใช้งานต้องมีความรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตน

4) รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดไว้ หรือเมื่อมีการแจ้งให้ปรับเปลี่ยนจากฝ่ายเทคโนโลยี

5.4 การควบคุมการเข้าถึงระบบ (System and application access control) เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลบนระบบสารสนเทศโดยไม่ได้รับอนุญาต ให้ปฏิบัติตามนโยบายดังต่อไปนี้

5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

1) มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน ได้แก่ เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้งาน ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมี เฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

2) บัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงระบบสารสนเทศในระดับพิเศษ หรือระดับสูง เช่น Root หรือ Administrator จะได้รับการมอบหมายให้แก่ผู้ดูแลระบบเท่านั้น จะไม่อนุญาตให้ผู้ดูแลส่งต่อข้อมูลให้กับผู้อื่น หรือข้อมูลผู้มีสิทธิสูงที่สร้างขึ้นมาเพื่อใช้ในการตั้งค่าระบบ จะต้องไม่ต้องการตั้งค่าสำหรับการ Remote ได้

3) บุคคลภายนอก ต้องมีการร้องขอการเข้าใช้ แสดงความยินยอมปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทอย่างเคร่งครัด และได้รับการอนุมัติจากหัวหน้าส่วนงานที่ควบคุม หรือหัวหน้าหน่วยงานฝ่ายเทคโนโลยี ก่อนที่จะได้รับ

อนุญาตให้เข้าถึงระบบสารสนเทศของบริษัทฯ ตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

5.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)

1) การเข้าถึงระบบปฏิบัติการจะต้องผ่านการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัยตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

5.5 การควบคุมการเข้าถึงเครือข่าย (Network Access Control) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

5.5.1 ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- 1) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- 2) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- 3) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- 4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
- 5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ
- 6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
- 7) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน
- 8) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

9) การระบุอุปกรณ์เครือข่าย

- a. ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- b. อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- c. ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- d. กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ที่สามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- e. อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
- f. กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อเว้นว่างจากการใช้งานเป็นเวลานาน

5.6 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงานในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น สามารถกำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน ดังนี้

- 5.6.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
- 5.6.2 หลังจากระบบติดตั้งเสร็จ ต้องมีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเชื่อมต่อการเปลี่ยนรหัสผ่านของผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที
- 5.6.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง
- 5.6.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
- 5.6.5 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- 5.6.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงวันแต่จะได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยี
- 5.6.7 ซอฟต์แวร์ที่บริษัท ใ้มีลิขสิทธิ์ ผู้ใช้งานสามารถใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

- 5.6.8 ซอฟต์แวร์ที่บริษัทจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น
- 5.6.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัท เพื่อประโยชน์ทางการค้า
- 5.6.10 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
- 5.6.11 ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

5.7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยมีการจัดการดังนี้

- 5.7.1 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวตามรอบ
- 5.7.2 ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- 5.7.3 ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

หมวดที่ 6. การจัดการชั้นความลับของสารสนเทศ (Information Classification Polity)

เพื่อให้ทรัพย์สินสารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

6.1 ชั้นความลับของสารสนเทศ (Classification of information)

1) กำหนดระดับความสำคัญ และกำหนดชั้นความลับ เพื่อป้องกันสารสนเทศให้มีความปลอดภัย โดยจัดแบ่งลำดับชั้นความลับของข้อมูลเป็น

- ข้อมูลลับที่สุด (Top Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หรือ ใช้ภายใน (Internal Use) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หรือ สาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่
ทั่วไปได้

2) ทรัพย์สินสารสนเทศ ซึ่งทำซ้ำมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ให้ถือว่าชั้น
ความลับเดียวกับต้นฉบับ

6.2 การบ่งชี้สารสนเทศ (Labeling of information) ต้องจัดให้มีวิธีการจัดทำ และจัดการป้ายชื่อทรัพย์สิน

6.2.1 การจัดการทรัพย์สิน (Handling of assets)

1) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นและได้รับการยกเว้น เพื่อใช้ใน
การปฏิบัติงาน

2) ข้อมูลที่เป็นข้อมูลลับต้องไม่เปิดเผยต่อบุคคลภายนอก ยกเว้นในกรณีที่มีการเปิดเผยนั้น
ครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

3) หากส่งผ่านข้อมูลที่เป็นข้อมูลลับผ่านเครือข่ายต้องป้องกันข้อมูลอย่างเหมาะสม ได้แก่
การปกป้องด้วยรหัสผ่าน หรือ การเข้ารหัสข้อมูล

4) ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมด ทั้งที่เก็บรักษาอยู่ใน
เครื่อง

คอมพิวเตอร์แม่ข่ายที่ดูแลโดยฝ่ายเทคโนโลยี จะได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อ
ประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใดๆ เกิดขึ้น ตัวอย่างเช่น การติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น

หมวดที่ 7. การเข้ารหัสข้อมูล (Cryptography)

7.1 การเข้ารหัสข้อมูล (Cryptographic controls) เพื่อให้ใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล
ป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

7.1.1 นโยบายการใช้นโยบายการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

1) ข้อมูลส่วนบุคคลของลูกค้าและลูกจ้างจะมีการควบคุมการเข้าถึง หรือเข้ารหัสข้อมูล
ตามข้อกำหนด ระเบียบ และกฎหมายที่เกี่ยวข้อง

2) การเข้ารหัสสื่อบันทึกข้อมูล (Disk Encryption)

สื่อบันทึกข้อมูลที่อยู่ภายใน เช่น (Hard disk, SSD) ที่มีข้อมูลขององค์กรบันทึกอยู่ จะ
ได้รับการเข้ารหัสป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ได้แก่ การจัดทำ BitLocker เข้ารหัสเพื่อ
ป้องกันการนำ Hard disk ไปติดตั้งเครื่องอื่น เพื่อทำการคัดลอกข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการ
จัดทำจะเป็นการเข้ารหัสโดยฝ่ายเทคโนโลยี

7.1.2 การบริหารจัดการกุญแจ (Key management)

1) มีการจัดทำแนวปฏิบัติการใช้งานกุญแจเพื่อเข้าห้องควบคุมหลัก และเก็บรักษา หรือ
ระบบการเข้าใช้งาน

2.) มีการจัดการระบบการเข้าใช้งานเฉพาะผู้ที่สามารถเข้าได้ โดยจะทำการสร้างเมื่อได้รับ
มอบหมายงานที่ต้องเข้าดำเนินการสม่ำเสมอ และลบออกเมื่อหมดสิทธิการเป็นพนักงาน หรือต้องมี

การบริหารจัดการวิธีการเข้าใช้ สำหรับผู้ที่ไม่มียุติสิทธิ์เข้า ได้แก่ ระบบการอ่านลายนิ้วมือ ระบบการอ่านใบหน้า

หมวดที่ 8. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

8.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas) เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

8.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)

- 1) มีการแบ่งพื้นที่อย่างชัดเจน และมีการควบคุมเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศที่มีความสำคัญ
- 2) มีการจัดทำแผนผังแสดงตำแหน่งและพื้นที่แต่ละชนิดและประกาศให้ผู้เกี่ยวข้องทราบ
- 3) มีการดูแลรักษาสภาพแวดล้อมของพื้นที่ให้เป็นไปตาม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

8.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

- 1) มีการควบคุมให้เฉพาะผู้ที่มีสิทธิ์ หรือผู้ที่ได้รับอนุญาตสามารถเข้าออกในพื้นที่
- 2) มีการกำหนดสิทธิ์ และช่วงเวลาในการผ่านเข้าออกพื้นที่
- 3) มีการบันทึกการผ่านเข้าออกในพื้นที่ที่สำคัญ
- 4) ไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นได้มีการร้องขอ อนุญาตให้เข้าและสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

8.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities)

- 1) จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก
- 2) เจ้าหน้าที่จะต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ ได้รับการปิดล็อก อย่างเหมาะสม และถูกดูแลรักษาไว้อย่างปลอดภัย
- 3) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในที่ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด

4) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

5) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่ บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการและเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

6) กรณีที่ต้องมีการเคลื่อนย้าย ต้องมีการแสดงความจำนงค์ วัตถุประสงค์ และแจ้งรายละเอียดตามขั้นตอนปฏิบัติที่กำหนด โดยจะถือว่าผู้ที่แจ้งความจำนงค์ตามเอกสาร เป็นผู้รับผิดชอบต่อทรัพย์สินเท่านั้น

8.1.4 การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external environmental threats)

- 1) มีวิธีป้องกันจากการทำลายของธรรมชาติเช่น ลม ฝน หรือน้ำท่วมหรือคนที่อาจจะเกิดขึ้น
- 2) มีระบบป้องกันไฟไหม้ อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน
- 3) มีระบบป้องกันไฟฟ้าขัดข้องให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ
- 4) มีระบบควบคุมความชื้นที่เหมาะสม โดยมีการตั้งอุณหภูมิเครื่องปรับอากาศและการตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะของระบบคอมพิวเตอร์

8.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)

- 1) หากพบสิ่งผิดปกติ หรือการละเมิดความมั่นคงปลอดภัย จะต้องแจ้งให้ผู้บังคับบัญชาทราบ
- 2) ในบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยต้องติดประกาศแจ้งเตือน เช่น "ห้ามเข้าก่อนได้รับอนุญาต"

8.2 อุปกรณ์ (Equipment) เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

8.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment siting and protection)

- 1) การจัดตั้ง หรือการจัดวางอุปกรณ์ทรัพย์สินสารสนเทศ อุปกรณ์ใดที่มีความสำคัญสูงต้องจัดวางในที่ที่เข้าถึงได้ยาก มีการคัดกรองการเข้าถึง

8.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

- 1) อุปกรณ์ที่มีความสำคัญสูงควรติดตั้งระบบป้องกันความล้มเหลวของอุปกรณ์ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศสำรอง ระบบดับเพลิงเป็นต้น
- 2) กรณีในส่วนของบริเวณของสาขา จะไม่อนุญาตให้ผู้ไม่มีส่วนเกี่ยวข้องหรือได้รับอนุญาตเข้าบริเวณที่เกี่ยวข้องกับระบบการขาย

8.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

- 1) การเดินสายสัญญาณต้องแยกท่อเพื่อป้องกันสัญญาณรบกวน
- 2) ต้องมีการทำป้ายสายสัญญาณชัดเจน และเมื่อมีการเปลี่ยนแปลงต้องมีการปรับปรุงป้ายสายสัญญาณให้ถูกต้อง

8.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

- 1) ต้องจัดให้มีการบำรุงรักษาอุปกรณ์เพื่อให้มีสภาพพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง หรือมากกว่าตามระดับความสำคัญ
- 2) มีการเข้าบำรุงรักษาอุปกรณ์ให้กับหน้าสาขาปีเว้นปี (2 ปี/ครั้ง) หรือตามการแจ้งปัญหา และมีความจำเป็นที่ต้องเข้าบริการ

8.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of assets)

- 1) ห้ามนำทรัพย์สินสารสนเทศออกนอกพื้นที่ก่อนได้รับอนุญาตจากผู้รับผิดชอบ และต้องมีขั้นตอนในการตรวจสอบและติดตาม
- 2) กรณีที่มีการนำทรัพย์สินออกโดยไม่ได้รับอนุญาต และไม่มีหัวหน้าหน่วยงานทราบ ถือว่ามีความผิด โดยฐานความผิดให้มีการพิจารณาตามความเหมาะสม ซึ่งมีฝ่ายกำกับฯ ดูแลและร่วมพิจารณา
- 3) กรณีนำทรัพย์สินออกนอกพื้นที่ และมีเหตุอันเป็นความเสียหาย ทางบริษัทฯ จะไม่มีส่วนรับผิดชอบกับความผิดอันเกิดจากเหตุ

8.2.6 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)

- 1) ข้อมูลที่เก็บอยู่บนสื่อบันทึกข้อมูล หากไม่มีการใช้งานแล้วต้องทำลายให้สิ้นซาก โดยให้เป็นไปตามแนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล
- 2) ก่อนการทำลายสื่อ หรือจำหน่ายสื่อออกจากองค์กร ต้องมีการตรวจสอบโดยอย่างน้อยฝ่ายเทคโนโลยี และฝ่ายบัญชีที่ดูแลเรื่องทรัพย์สินก่อน เพื่อให้มั่นใจว่า ไม่มีส่วนของข้อมูลหลุดออกจากองค์กร

หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

9.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities) เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

9.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

- 1) มีคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับสารสนเทศที่สำคัญของหน่วยงาน เพื่อป้องกันการปฏิบัติงานด้านสารสนเทศที่ผิดพลาด
- 2) มีการส่งมอบทรัพย์สินให้กับผู้ใช้งาน หรือผู้ที่รับผิดชอบโดยตรงเป็นลายลักษณ์อักษร

9.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

- 1) กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น มีการขออนุมัติจากผู้บังคับบัญชา หรือกลุ่มงานที่เกี่ยวข้องก่อนดำเนินการ
- 2) มีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงข้อมูลสารสนเทศ
- 3) มีการรับอนุญาตและเห็นชอบจากหน่วยงานที่เป็นเจ้าของ ก่อนมีการปรับเปลี่ยน

9.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)

- 1) มีการตรวจสอบติดตามทรัพยากรของระบบ เช่น CPU Memory Hard disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
- 2) มีการประเมินอัตราการเพิ่มของข้อมูล เพื่อนำมาวิเคราะห์กระบวนกรเพิ่มทรัพยากรหรือกระบวนกรจัดเก็บ (Backup)
- 3) มีการนำข้อมูลที่ไม่ใช้แล้วออกจากระบบ หรือทำลายในกรณีที่ไม่ใช้แล้ว เพื่อดำเนินงานให้มีประสิทธิภาพ

9.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน

(Separation of development, testing and operational environments)

- 1) ในระบบที่มีความสำคัญสูง จะมีการแยกระบบการพัฒนา ออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลที่ผิดพลาด หรือโดยไม่ได้รับอนุญาต
- 2) ก่อนทำการนำระบบขึ้นใช้จริง ต้องมีการทดสอบและยินยอมรับผลการทดสอบ จากหน่วยงานที่เกี่ยวข้อง โดยอย่างน้อยต้องมีฝ่ายเทคโนโลยี และฝ่ายกำกับกิจการของบริษัท

9.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

9.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against virus & malware)

- 1) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่อง ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์
- 2) ปรับปรุง Patch และ Hot Fix ของ Application อย่างสม่ำเสมอ โดยสามารถดาวน์โหลด Patch และ Hot Fix ต่างๆ จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ไขปัญหาช่องโหว่ เป็นต้น
- 3) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตหรืออุปกรณ์ต่อพ่วงจะต้องทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัส (Antivirus) ก่อนการรับส่งข้อมูลทุกครั้ง
- 4) ปรับปรุง Patch และ Hot Fix ของระบบปฏิบัติการอย่างสม่ำเสมอ โดยดาวน์โหลด Patch และ Hot Fix จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ไขปัญหาช่องโหว่ ได้แก่ การปรับปรุง Patch ระบบปฏิบัติการ (Windows Update) เมื่อผู้ให้บริการจัดส่งให้ หรือการปรับปรุงระบบป้องกันไวรัสเฉพาะ

- 5) เครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์แบบพกพาทุกเครื่อง จะเปิดการใช้งานระบบป้องกันการเข้าออกของข้อมูล (Firewall) เพื่อตรวจสอบการเข้าออกของข้อมูลและกำหนดให้อนุญาตและไม่อนุญาต
- 6) มีการป้องกัน การเฝ้าระวังความไม่ประสงค์ดีโดยโปรแกรมที่ยอมรับ หรือผ่านโครงสร้างพื้นฐานด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ
- 7) มีการจัดทำรายงานความผิดปกติ ความไม่หวังดีและนำเสนอผู้บริหารฝ่ายเทคโนโลยีเป็นประจำทุกเดือน เพื่อนำเสนอผู้บริหารระดับสูงเป็นรายไตรมาส
- 8) มีการติดตามข้อมูล ข่าวสารจากหน่วยงานภายนอก เกี่ยวกับความปลอดภัย เพื่อนำมาทำการปรับปรุงให้ระบบภายในองค์กร มีความทันสมัย และพร้อมรับสถานการณ์ที่ไม่ปกติได้อย่างสม่ำเสมอ

9.3 การสำรองข้อมูล (Backup) เพื่อป้องกันการสูญหายของข้อมูล และให้มั่นใจว่าระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

9.3.1 ระเบียบวิธีปฏิบัติการสำรองและกู้คืนข้อมูล (Information backup and recovery policy)

- 1) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการจะมีการสำรองข้อมูล ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล
- 2) มีการสำรวจข้อมูล และจัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล
- 3) ระบบที่มีความสำคัญสูงจะมีการจัดให้มีการสำรองข้อมูลมาก และมีการสำรองข้อมูลภายนอกสำนักงาน หรือข้อมูลอยู่คนละส่วนของระบบ (Offsite)
- 4) มีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ
- 5) มีการสุ่มทดสอบข้อมูลที่สำรองไว้
- 6) มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ 1 ครั้ง
- 7) หากต้องมีการกู้คืนข้อมูลให้ดำเนินการกู้คืนข้อมูลตาม ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

9.4 การบันทึกข้อมูล Log และการเฝ้าระวัง (Logging and Monitoring) เพื่อให้มีการบันทึกเหตุการณ์ และจัดทำหลักฐาน

9.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging)

- 1) ฝ่ายเทคโนโลยีจะมีการจัดเก็บข้อมูลบันทึกกิจกรรมของผู้ใช้งาน หรือมีการนำเก็บกับผู้ให้บริการที่ผ่านกระบวนการคัดสรรแล้ว เพื่อใช้ติดตามกรณีเกิดเหตุความมั่นคงปลอดภัย
- 2) มีการจัดเก็บล็อก อย่างน้อย 90 วัน ตาม พรบ. ความมั่นคงปลอดภัยคอมพิวเตอร์

8.4.2 การป้องกันข้อมูลล็อก (Protection of log information)

- 1) อุปกรณ์บันทึกล็อกและข้อมูลการล็อกสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- 2) กรณีที่ต้องการนำล็อกออกมา จะต้องมีการแจ้งความจำนงค์ ร้องขอโดยผ่านความเห็นชอบจากหัวหน้าหน่วยงาน และหน่วยงานควบคุมและกำกับดูแล

8.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)

- 1) มีการตรวจสอบกิจกรรมการดำเนินงานของผู้ดูแลระบบ และมีการทบทวนสม่ำเสมอ
- 2) มีการรายงานทบทวนล็อกถึงกิจกรรมที่มีความสำคัญ หรือมีความผิดปกติให้กับหัวหน้าฝ่ายเทคโนโลยี หรือฝ่ายกำกับดูแล หรือผู้บริหารระดับสูง ทุกเดือน เช่น กระบวนการปรับปรุงผู้มีสิทธิสูง เป็นต้น

9.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

- 1) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องมีการตั้งเวลาให้ตรงกันโดยเทียบเวลาจากเซิร์ฟเวอร์

9.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software) เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง และมีประสิทธิภาพ

8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)

- 1) จะมีการติดตั้งเฉพาะที่ซอฟต์แวร์ที่จำเป็นและมีลิขสิทธิ์ ไม่ผิดกฎหมายในการให้บริการ

9.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) วัตถุประสงค์เพื่อป้องกันการรั่วไหลของข้อมูลจากช่องโหว่ทางเทคนิค

9.6.1 การจำกัดการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Restrictions on software installation)

- 1) ระบบที่ให้บริการจะทำการ Patch ซอฟต์แวร์อย่างสม่ำเสมอ
- 2) มีการลบข้อมูลผู้ใช้ที่ไม่จำเป็นออกจากระบบ เช่น Test, Training
- 3) มีการปิด Service ที่ไม่ได้ใช้งาน
- 4) ปิดพอร์ต (Port) ที่ไม่ได้ใช้งาน
- 5) มีการติดตั้งระบบรักษาความปลอดภัย และเฝ้าระวังความไม่ประสงค์ดีเสมอ
- 6) ซอฟต์แวร์ใดไม่ได้ใช้งาน และไม่มี ความจำเป็นกับบริษัท พนักงานฝ่ายปฏิบัติงาน

เทคโนโลยีจะทำการลบออก

- 7) ไม่อนุญาตให้มีการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ในการปฏิบัติงาน

9.6.2 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

- 1) มีการตรวจสอบช่องโหว่ของโปรแกรมที่สำคัญ ที่ผ่านการอนุมัติจากผู้บริหาร หรือฝ่ายกำกับ อย่างน้อย 2 ปี ต่อ 1 ครั้ง

9.6.3 หน่วยงานบริหารงานด้านเทคโนโลยีสารสนเทศ ต้องมีการจัดการตรวจสอบช่องโหว่ (Vulnerability Assessment) ด้านเครือข่ายอย่างน้อย 2 ปีต่อ 1 ครั้ง เพื่อตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และจัดทำรายงานเป็นผลชี้วัดความปลอดภัย

9.6.4 หน่วยงานบริหารงานด้านเทคโนโลยีสารสนเทศ ควรจัดการตรวจสอบเจาะโปรแกรม (Penetration Testing – Pen Test) ที่เกี่ยวกับข้อมูลลูกค้า อย่างน้อยสองปีครั้ง หรือเมื่อมีการปรับเปลี่ยนระบบ เพื่อตรวจสอบและจัดทำรายงานให้อยู่ลักษณะที่สามารถนำเสนอให้กับหน่วยงานรักษาความปลอดภัยทางด้านเทคโนโลยีแห่งชาติ เมื่อเกิดการเจาะระบบจากผู้ไม่ประสงค์ดี (Hacker) ได้

9.7 การบริหารจัดการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center - SOC) คือ หน่วยงานเทคโนโลยีสารสนเทศ จัดการหรือสรรหาผู้ให้บริการด้านการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ คอยทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมินตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

การจัดการของศูนย์เฝ้าระวังความมั่นคงปลอดภัย จะสามารถป้องกันการโจมตีตามพื้นฐานความปลอดภัยทั่วไป และจากการตกลงร่วมกันกับฝ่ายเทคโนโลยี เพื่อให้การป้องกันมีประสิทธิภาพสูงสุด

หมวดที่ 10 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

10.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management) เพื่อให้มีการป้องกันสารสนเทศในเครือข่าย และอุปกรณ์ประมวลผลสารสนเทศ

10.1.1 มาตรการเครือข่าย (Network controls)

1) กำหนดนโยบายการควบคุมการเข้าถึงเครือข่าย และบริการเครือข่ายให้มีความมั่นคงปลอดภัยโดยให้เป็นไปตามแนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย และแนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

10.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

1) ผู้บริหารมีการกำหนดระดับความต้องการสำหรับบริการเครือข่าย เช่น ร้านค้าต้องการเข้าถึงระบบกล้องวงจรปิดหรือไม่

10.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)

1) ผู้ดูแลระบบมีการจัดแบ่งเครือข่ายระหว่างการใช้งานภายในและผู้ใช้งานนอกที่ติดต่อกับบริษัท โดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

10.2 การถ่ายโอนสารสนเทศ (Information transfer) เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

10.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)

1) การใช้บริการสารสนเทศจากหน่วยงานภายนอก ให้เป็นไปตามแนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ โดยจะมีการร้องขอข้อมูลการเชื่อมต่อเข้าระบบก่อน ถึงจะสามารถเชื่อมต่อเข้ามาใช้งานระบบภายในได้

10.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer)

1) ผู้ดูแลระบบจะควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ

- การรักษาความลับ (Confidentiality)
- การรักษาความถูกต้องของข้อมูล (Integrity)
- การรักษาความพร้อมที่จะให้บริการ (Availability)

10.2.3 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)

1) ต้องจัดให้มีการลงนามในสัญญาระหว่างหน่วยงานและหน่วยงานภายนอกทุกครั้งที่มีผู้ให้บริการใหม่ว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA)

หมวดที่ 11 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

11.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems) เพื่อให้ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย ให้ปฏิบัติตามนโยบายดังนี้

11.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security requirements analysis and specification)

1) มีการกำหนดความต้องการด้านความมั่นคงปลอดภัยก่อนจะพัฒนาขึ้นมาใช้งานหรือซื้อมาใช้งาน

2) มีการทดสอบหรือศึกษา ทำความเข้าใจ เปรียบเทียบก่อนทำการตัดสินใจนำมาใช้งานหรือซื้อมาใช้งาน โดยต้องได้รับความยินยอมจากหน่วยงานที่ร้องขอ และ/หรือคณะกรรมการที่มีส่วนเกี่ยวข้อง

11.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

1) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการดักฟัง และการเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

11.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

1) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

11.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes) เพื่อให้ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ ให้ปฏิบัติตามนโยบายดังต่อไปนี้

11.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

1) ผู้พัฒนาระบบสารสนเทศจะมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง โดยจะมีการอนุมัติโดยผู้มีอำนาจเสมอ

11.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

1) ผู้พัฒนาระบบสารสนเทศจัดทำแนวปฏิบัติการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ

11.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes)

1) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่างๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่องานและความมั่นคงปลอดภัย

11.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages)

1) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

11.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

1) มีการนำหลักการวิศวกรรมระบบมาประยุกต์ใช้กับงานการพัฒนาระบบ เช่น

- นำระบบงานที่สำคัญไปอยู่ภายใต้การควบคุมของระบบ Firewall
- การออกแบบด้านความมั่นคงปลอดภัยต้องให้ง่ายสำหรับการทำความเข้าใจ

11.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคง (Secure development environment)

1) หากมีความจำเป็นต้องให้หน่วยงานภายนอกเข้ามาพัฒนาระบบภายในหน่วยงาน จะมีการกำหนดสภาพแวดล้อมที่มีความมั่นคงปลอดภัย โดยมีการจัดทำขั้นตอนการขอเข้าใช้งาน และ

กำหนดสภาพแวดล้อมการใช้งาน เช่น ตัดการเชื่อมต่อเครือข่ายออกสู่ภายนอกเพื่อป้องกันการนำข้อมูลลับออกสู่ภายนอก

- 2) มีการแบ่งสิทธิตามหน้าที่การทำงานอย่างชัดเจน เช่น ผู้พัฒนาระบบ ผู้ดูแลฐานข้อมูล
- 3) มีการตรวจสอบประวัติของหน่วยงานภายนอกที่มารับจ้าง
- 4) หน่วยงานภายนอกต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยของหน่วยงานตามที่ได้ประกาศจากทางบริษัทฯ

11.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development)

- 1) มีการประชุมติดตาม กิจกรรมการพัฒนาระบบอย่างสม่ำเสมอ
- 2) หากพบการละเมิดความมั่นคงปลอดภัยต้องแจ้งให้ผู้บังคับบัญชาทราบทันที
- 3) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก
- 4) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น
- 5) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง
- 6) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ
- 7) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ
- 8) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

11.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

- 1) การทดสอบด้านความมั่นคงปลอดภัยต้องทำการทดสอบการใช้งานในช่วงของการพัฒนา หากไม่ผ่านการทดสอบต้องแก้ไขให้แล้วเสร็จก่อนการส่งมอบ หรือมีการยินยอมจากผู้มีอำนาจอนุมัติให้ใช้งาน

11.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

- 1) การทำงานของฟังก์ชันทุกฟังก์ชันการทำงาน มีการทดสอบการทำงานได้ถูกต้อง และได้รับการยอมรับจากผู้ใช้งานหรือผู้รับผิดชอบระบบ

หมวดที่ 12 การบริหารงานและความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

12.1 ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Technology Security in supplier relationship) เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอกปฏิบัติตามนโยบายดังต่อไปนี้

12.1.1 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Technology Security Policy for Supplier Relationships) ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ให้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร

12.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)

- 1) ระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ผู้ใช้งานเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ต้องมีการร้องขอและอนุญาตให้สามารถเข้าถึงได้
- 2) มีการประเมินและคัดเลือกผู้ให้บริการ โดยขั้นตอนอย่างน้อยดังนี้
 - a. มีพื้นฐาน หรือ Background ในส่วนงานที่เกี่ยวข้อง เป็นที่น่าเชื่อถือ
 - b. ไม่เป็นบริษัทที่มีประวัติเสียหาย
 - c. มีการคัดสรรจากผู้ให้บริการอย่างน้อย 3 บริษัท
 - d. ผู้ให้บริการ มีความเข้าใจในส่วนงานที่จะนำเสนอ สามารถให้คำปรึกษา และมีประสบการณ์ในงานที่เกี่ยวข้องเป็นอย่างดี
 - e. มีการบันทึกและยอมรับข้อตกลงในการดำเนินการ โดยเห็นชอบจากคณะกรรมการและฝ่ายกฎหมายของบริษัท
 - f. มีกระบวนการแจ้งความคืบหน้าในการดำเนินการ
- 3) มีการประเมินความเสี่ยงในการดำเนินการเป็นระยะ อย่างน้อย ในทุกๆระยะที่มีความสำคัญ

12.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

(Information and communication technology supply chain)

- 1) ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ต้องสื่อสารถึงห่วงโซ่ผู้ให้บริการหรือผู้รับบริการภายนอกทั้งหมดที่เข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร

12.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management) เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการของผู้ให้บริการภายนอก ให้ปฏิบัติตามนโยบายต่อไปนี้

12.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of supplier services)

1) ในข้อตกลงการให้บริการ กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

12.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing changes to supplier services)

1) หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการ สำหรับระบบที่สำคัญ จะต้องจัดทำ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย และจัดทำเป็นลายลักษณ์อักษร

หมวดที่ 13 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Incident Management)

13.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Incident Management) เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการ เหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้ได้รับทราบให้ปฏิบัติตามนโยบาย ดังต่อไปนี้

13.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

1) มีการกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยของหน่วยงาน และมีความเป็นระบบระเบียบที่ดี โดยให้เป็นไปตามแนว ปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

13.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Reporting Information Technology Security events)

1) มีการกำหนดช่องทางการติดต่อเพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยอย่าง ชัดเจน

13.1.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Reporting Information Technology Security weaknesses)

1) หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องรายงานเหตุการณ์ดังกล่าวต่อผู้รับผิดชอบทันที

13.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Assessment and decision on Information Technology Security events)

1) ก่อนการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยจะมีการตรวจสอบให้ชัดเจน และสอบถามกับผู้ร่วมงานอย่างน้อย 1 ท่าน

13.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Response to information security incidents)

1) กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

2) มีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น เพื่อจะได้เรียนรู้และเตรียมการป้องกันในอนาคต

13.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)

1) มีการเก็บรวบรวมและจัดเก็บหลักฐานตามกฎหมายหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางกฎหมาย เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรือกฎหมายอาญาหรือตามกฎหมายอื่นที่เกี่ยวข้อง

หมวดที่ 14 การบริหารจัดการความมั่นคงปลอดภัยเพื่อสร้างความต่อเนื่องขององค์กร

(Information Technology Security aspects of business continuity management)

14.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Incident Management) เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากวิกฤตหรือภัยพิบัติให้ปฏิบัติตามนโยบายดังนี้

14.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Planning Information Technology Security continuity policy)

1) ผู้ดูแลระบบมีการจัดทำแผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) ตามแนวปฏิบัติการสำรองและการกู้คืนข้อมูล

14.1.2 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Risk assessment information policy)

1) มีดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

14.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Verify, Review and Evaluate Information Technology Security continuity)

1) มีการทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ 1 ครั้ง

14.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies) เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศให้ปฏิบัติตามนโยบายดังนี้

14.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

1) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้เพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ตามความจำเป็นหรือความต้องการที่กำหนดไว้

2) ระบบ network มีการสำรองหรือ จัดหาช่องทางเตรียมไว้เพื่อให้ระบบกลับคืนมาในระยะเวลาที่ยอมรับได้และมีความเสียหายน้อยที่สุด

3) จุดที่มีความเสี่ยงสูง (single point of failure) จะมีการประเมิน และกำจัดให้เป็นศูนย์

หมวดที่ 15 ความสอดคล้อง (Compliance)

15.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with legal and contractual requirements)

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และตามความต้องการด้านความมั่นคงปลอดภัย ให้ปฏิบัติตามนโยบายดังต่อไปนี้

15.1.1 การระบุกฎและความต้องการในสัญญาที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)

1) จัดทำประกาศนโยบาย และแนวปฏิบัติ คู่มือการใช้งานสารสนเทศ พร้อมทั้งเผยแพร่ทางเว็บไซต์ <https://HRGuru.zengroup.co.th> และประกาศผ่านช่องทางที่บริษัทกำหนด เช่น Email หรือป้ายประกาศ

2) ผู้ดูแลระบบจะจัดให้มีการอบรมที่สอดคล้องกับการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

3) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็นทรัพย์สินของ บริษัทฯ (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทฯ สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

4) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามวัตถุประสงค์ในการปฏิบัติงานและถูกต้องตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

5) ห้ามเจ้าหน้าที่ฝ่ายเทคโนโลยีและพนักงานบริษัทฯ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

6) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใดๆ ออกนอกประเทศ ต้องไม่ขัดต่อข้อกำหนดใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

14.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights)

1) ต้องปฏิบัติตาม ข้อกำหนดที่ระบุไว้ใน ลิขสิทธิ์ (Copy right) การใช้งานซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมี การลงทะเบียนเพื่อใช้งานซอฟต์แวร์และต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์

15.1.3 การป้องกันข้อมูล (Protection of records)

1) ห้ามผู้ใช้งานทำซ้ำ เผยแพร่ ข้อมูลที่เป็นการละเมิดลิขสิทธิ์ หรือซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กร

15.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)

1) บริษัทมีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจของบริษัทโดยไม่ตรวจสอบจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่บริษัทมีภาระผูกพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ บริษัทสงวนสิทธิในการใช้ระบบเฝ้าระวังเพื่อตรวจสอบเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์ และกลั่นกรองหรือระงับการเผยแพร่ที่ขัดโมฆะ ตลอดจนสงวนสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์ เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใดๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือร้องขอจากผู้บริหารระดับสูง(ตั้งแต่ระดับ M ขึ้นไป) เป็นลายลักษณ์อักษร

15.2 การทบทวนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security reviews) เพื่อให้มีการปฏิบัติตามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสอดคล้องกับนโยบาย แนวปฏิบัติข้อกำหนดขององค์กรให้ปฏิบัติตามนโยบายดัง นโยบายต่อไปนี้

15.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Independent review of information security)

1) นโยบาย แนวปฏิบัติ ข้อกำหนด มาตรการต่าง ๆ ต้องมีการทบทวนตามรอบระยะเวลาที่กำหนด

15.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)

1) หน่วยงานมีการตรวจสอบ สอดส่อง ขั้นตอนปฏิบัติที่อยู่ภายใต้การดำเนินงานของตนเองโดยเทียบกับนโยบายมาตรฐาน

15.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

1) การตั้งค่าการทำงานของระบบต้องได้รับการทบทวนอย่างสม่ำเสมอ เพื่อมุ่งไปยังการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

2) การตั้งค่าการทำงานของระบบ มีการสอบทานจากผู้เชี่ยวชาญ หรือหน่วยงานความมั่นคงปลอดภัย หรือที่ปรึกษา ในกรณีที่มีความไม่เข้าใจ หรือความไม่ชัดเจน

หมวดที่ 16 นโยบายความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security Policy)

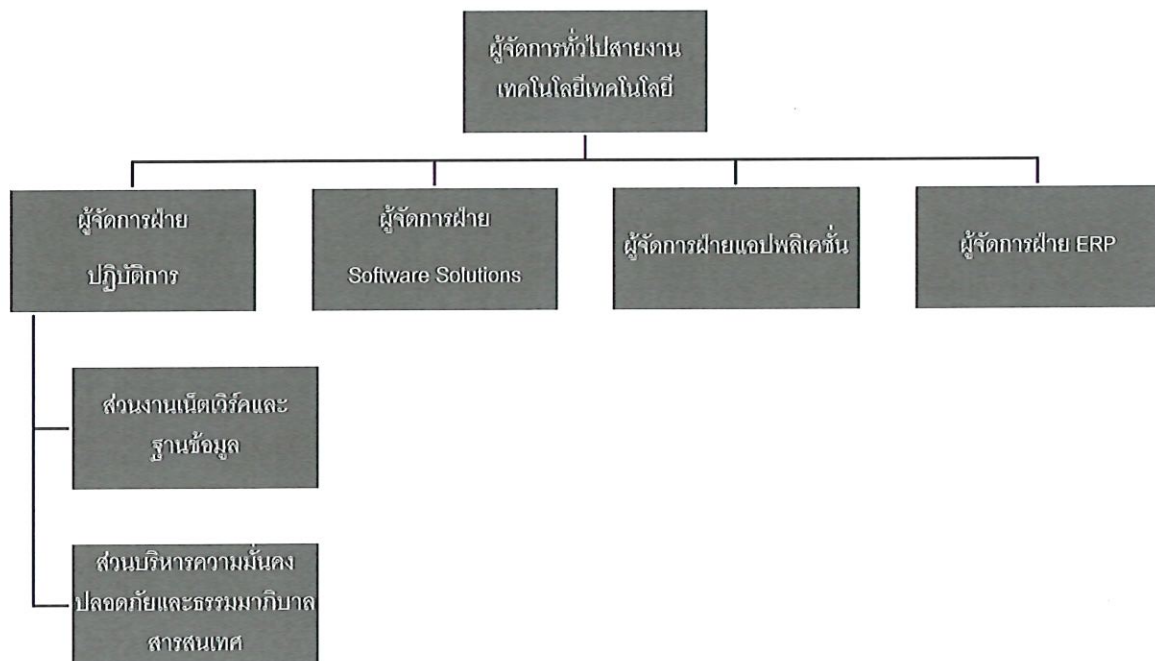
เพื่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ขององค์กร และการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อการป้องกันจากภัยคุกคามจากภายนอก ที่มีผู้ใช้อินเทอร์เน็ตมากขึ้นทุกช่องทาง และทุกหน่วยงาน ซึ่งจะเพิ่มเติมจากหัวข้ออื่นในเรื่องที่เกี่ยวข้อง ดังนี้ การเผยแพร่ข้อมูล หรือการนำข้อมูลมาใช้ในการดำเนินงาน การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายกับองค์กร โดยมีสาระสำคัญดังนี้

- 16.1 ให้มีคณะทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตัวแทนจากทางหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และกำหนดหน้าที่ความรับผิดชอบพร้อมทั้งวิธีการบริหารจัดการ
- 16.2 พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล และติดตามกฎหมายและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง และพิจารณาการปฏิบัติตามให้สอดคล้อง
- 16.3 ให้มีการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ โดยการประเมินจากภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) ความเป็นไปได้ (Likelihoods) และผลกระทบ (Impact) ต่อธุรกิจ รวมทั้งให้มีการจัดการความเสี่ยง ที่มีความสอดคล้องกับการบริหารความเสี่ยงในระดับองค์กร โดยขอบเขตของการบริหารความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงสินทรัพย์และบุคลากรทั้งหมดขององค์กร อีกทั้งหน่วยงานภายนอกที่เกี่ยวข้อง
- 16.4 สื่อความและจัดอบรมให้ความรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) เพื่อสร้างความตระหนักรู้ ความรับผิดชอบ และความเข้าใจการรับมือกับภัยคุกคามทางไซเบอร์ให้กับพนักงานอย่างน้อยปีละ 1 ครั้ง
- 16.5 ให้มีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุกด้านไซเบอร์ให้ครอบคลุมระบบสารสนเทศของบริษัท พร้อมทั้งจัดให้มีการเฝ้าระวัง และให้หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ ต้องรายงานข้อมูลภัยคุกคามด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างน้อยไตรมาสละครั้ง
- 16.6 ให้จัดทำแผนการตอบสนองเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อการจัดการเหตุการณ์ผิดปกติได้อย่างรวดเร็วและมีประสิทธิภาพ พร้อมทั้งลดผลกระทบต่อกระบวนการธุรกิจที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนการตอบสนองฯ อย่างน้อยปีละครั้ง
- 16.7 ให้จัดทำแผนฟื้นฟูหลังจากเกิดเหตุการณ์ผิดปกติ เพื่อลดผลกระทบต่อกระบวนการธุรกิจที่สำคัญ พร้อมทั้งทดสอบและทบทวนแผนฟื้นฟู เพื่อประเมินความถูกต้องและมีประสิทธิผลของแผน อย่างน้อยปีละ 1 ครั้ง

- 16.8 ให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ 1 ครั้ง

คณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยี

(Organization of Information Security)



ส่วนที่ 3

แนวปฏิบัติ (Procedure and Guide line)

แนวปฏิบัติการใช้งานสารสนเทศให้มั่นคงปลอดภัย

1. การใช้งานรหัสผ่าน นโยบายการจัดการรหัสผ่านที่ใช้งาน ผู้ใช้งานต้องปฏิบัติตามนี้

1.1. สำหรับระบบปฏิบัติการ

- 1.1.1. ผู้ใช้งานในส่วนของผู้ใช้งานออฟฟิศ ควรเปลี่ยนรหัสผ่านทุก 90 วัน หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน
- 1.1.2. ผู้ใช้งานในส่วนของผู้ปฏิบัติหน้าสาขา ที่ไม่มีสิทธิในการเข้าใช้งานเครื่องคอมพิวเตอร์ จะเปลี่ยนรหัสผ่านทุก 365 วัน (1 ปี) หรือเมื่อระบบแจ้งเตือนให้เปลี่ยนรหัสผ่าน
- 1.1.3. เลือกรหัสผ่านที่ปลอดภัย ตามนโยบายการตั้งรหัสผ่าน ของแต่ละระบบและรักษารหัสผ่านให้เป็นความลับอยู่ตลอดเวลา
- 1.1.4. ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ
- 1.1.5. ไม่ลักลอบใช้รหัสผ่าน หรือแคะรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น
- 1.1.6. รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

1.1. สำหรับระบบการขาย จะมีการจัดการที่ต่างออกไป เนื่องด้วยข้อจำกัดของระบบ โดยแยกตามแต่ละซอฟต์แวร์ ตามเอกสารการปฏิบัติงาน (Work instruction – WI) หมวด P015 - บทบาท/หน้าที่และลำดับขั้นตอนการเข้าถึงข้อมูล (Role/Responsibility and Access Right) และมีแนวทางปฏิบัติดังนี้

- 1.1.1. ผู้ใช้งานจะได้รับข้อมูลการเข้าระบบที่สามารถเข้าได้ ก็ต่อเมื่อเป็นพนักงานเรียบร้อยแล้ว หรือกรณีโปรแกรมเฉพาะ เมื่อได้รับความยินยอมจากหัวหน้างาน และได้รับการอนุมัติจากผู้มีอำนาจแล้วเท่านั้น
- 1.1.2. รหัสผ่านจะเป็นการสุ่มอัตโนมัติ และนำส่งให้หัวหน้างาน
- 1.1.3. ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ
- 1.1.4. ไม่ลักลอบใช้รหัสผ่าน หรือแคะรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น
- 1.1.5. รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

W. Thumtner

2. การถือครองรหัสผ่าน แบ่งออกเป็น 2 ประเภทตามการครอบครอง และสิทธิการเข้าใช้งานคือ
 - 2.1. ผู้ถือครองรหัสผ่านทั่วไป คือผู้ถือครองสำหรับผู้ใช้งานทั่วไป จะมีอำนาจหน้าที่ในการใช้งานรหัสผ่านของตนเองเท่านั้น ถือว่าเป็นข้อมูลลับที่สุดของตนเอง ห้ามไม่ให้บอกกล่าว หรือให้ผู้อื่นยืมไปใช้งาน โดยจะถือว่ามีความผิดสูง มีผลในการพิจารณาลงโทษ
 - 2.2. ผู้ถือครองรหัสผ่านสำหรับระบบที่มีสิทธิสูง คือผู้ดูแลรหัสผ่านสำหรับระบบต่างๆ เพื่อใช้ในการปรับปรุงแก้ไขระบบ ติดตั้งการใช้งาน หรือสร้าง แก้ไข ข้อมูลผู้ใช้ทั่วไปได้ ข้อมูลรหัสผ่านประเภทนี้ จะมีการปรับเปลี่ยนไม่บ่อยครั้ง หรือไม่ปรับเปลี่ยนเลย ข้อมูลรหัสผ่านจะต้องมีการจัดเก็บเป็นความลับ ให้กับฝ่ายที่ดูแลระบบของหน่วยงานเทคโนโลยีเท่านั้น โดยจะมีการเก็บเป็นเอกสารลายลักษณ์อักษรหรืออยู่ในรูปแบบไฟล์อิเล็กทรอนิกส์ ที่จัดอยู่ในประเภทความลับสูง กรณีที่ต้องมีการปรับเปลี่ยน สร้างใหม่ ต้องได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยี และเห็นพ้องจากหัวหน้าหน่วยงานเทคโนโลยี
 - 2.2.1. กรณีรหัสผ่านที่ใช้สำหรับระบบงาน จะมีการตั้งค่าไม่เหมือนกับประเภทผู้ใช้งานจริง ทั้งกรณีผู้ใช้งานทั่วไป และผู้มีสิทธิสูง โดยจะมีการตั้งค่าที่สำคัญคือ
 - 2.2.1.1. ชื่อผู้ใช้งาน จะไม่ใช่ ชื่อ และตามด้วยนามสกุล
 - 2.2.1.2. ไม่มีการหมดอายุของรหัสผ่าน
 - 2.2.1.3. มีการเสนออนุมัติจากหัวหน้าส่วนงานเทคโนโลยีก่อนใช้งาน
 - 2.2.1.4. รายละเอียดที่ไม่จำเป็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น เบอร์โทรศัพท์ หน่วยงาน
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ดูแล เพื่อป้องกันข้อมูลสำคัญสูญหาย
 - 2.1. ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิการใช้คอมพิวเตอร์และเครือข่ายโดยทันที หากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ
 - 2.2. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องจะมีการจัดการ screen saver จากศูนย์กลาง เพื่อจะทำการล็อคหน้าจอ และใช้รหัสในการเข้าใช้
 - 2.3. การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานจะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์ หรืออุปกรณ์สำนักงานนั้น
4. ต้องไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ
 - 4.1. มีการกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน
 - 4.2. เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องจะมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ
 - 4.3. ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้อุดูแลชั่วคราว

- 4.4. การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา, tablet, mobile device เมื่อปฏิบัติงานอยู่นอกสถานที่ ได้แก่
 - 4.4.1. การตั้งออกจากหน้าจอหลัก เมื่อไม่ได้ใช้งานในระยะเวลาสั้น เพื่อการล็อกหน้าจอ
 - 4.4.2. การใช้กุญแจล็อกที่เก็บเครื่องคอมพิวเตอร์หรืออุปกรณ์พกพาเพื่อป้องกันสูญหาย
 - 4.4.3. มีการเข้ารหัสหรือตั้งค่าการเข้าใช้งานโปรแกรมที่มีข้อมูลที่สำคัญไว้
- 4.5. ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ แต่ต้องใช้ด้วยความระมัดระวัง และหารือกับฝ่ายเทคโนโลยีก่อนเสมอ
 - 4.5.1. การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ
 - 4.5.2. ไม่อนุญาตให้ส่งผ่านข้อมูลลับผ่านเครือข่าย หากต้องส่งผ่านเครือข่ายต้องขออนุญาตจากผู้บังคับบัญชาทุกครั้ง และในกรณีที่ เป็นไฟล์แนบต้องเข้ารหัสด้วยรหัสผ่านทุกครั้ง
 - 4.5.3. การสำเนาข้อมูลขึ้นความลับต้องจดบันทึกจำนวนชุดที่สำเนา รายละเอียดผู้ดำเนินการทุกครั้ง
5. การทำลายสื่อบันทึกข้อมูลหรือข้อมูลลับให้เป็นไปตามแนวปฏิบัติในการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

แนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต และรวมความถึงการกำหนดหน้าที่ของผู้ใช้งาน การเข้าถึงเครือข่าย การใช้งานระบบสารสนเทศ การเฝ้าดูการใช้งานระบบสารสนเทศ และอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศของบริษัทฯ เป็นต้น

1. ผู้ดูแลระบบจะมีการกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ดังนี้
 - 1.1. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

- สิทธิอ่านอย่างเดียว
- สิทธิการเพิ่มข้อมูล
- สิทธิการแก้ไขข้อมูล
- สิทธิการลบข้อมูล
- สิทธิการอนุมัติ/อนุญาต
- ไม่มีสิทธิ

1.2. กำหนดการระดับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน ที่ได้กำหนดไว้

1.3. ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศจะต้องร้องขอเป็นลายลักษณ์อักษร และได้รับการพิจารณาจากผู้ดูแลระบบที่ได้รับมอบหมาย

1.4. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ไว้ ดังนี้

1.4.1. จัดแบ่งประเภทข้อมูลออกเป็น

1.4.1.1. ข้อมูลทั่วไปที่เปิดเผยได้

1.4.1.2. ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ได้แก่

1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำร้อง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

2) ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านธุรกิจข้อมูลการขาย เป็นต้น

1.4.2. จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 4 ระดับ

1.4.2.1. ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูลงบประมาณการเงินและบัญชี

1.4.2.2. ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลส่วนบุคคล ข้อมูลบุคลากร

1.4.2.3. ข้อมูลที่มีระดับความสำคัญปานกลาง

1.4.2.4. ข้อมูลที่มีระดับความสำคัญน้อย

หากข้อมูลที่นอกเหนือจากที่กำหนด การจัดระดับความสำคัญของข้อมูล ให้พิจารณาด้วยการประเมินมูลค่าความเสียหายต่อหน่วยงานหากข้อมูลมีปัญหา ไม่สมบูรณ์ แนวปฏิบัติในการพิจารณาจัดลำดับความสำคัญของข้อมูลมีดังนี้

ระดับความสำคัญ	มูลค่าความเสียหายที่ประเมินได้จากข้อมูลเมื่อมีปัญหา หรือไม่สมบูรณ์
ความสำคัญมากที่สุด	มีผลกระทบรุนแรงต่อการดำรงอยู่ของหน่วยงาน หรือปิดหน่วยงาน
ความสำคัญมาก	มีผลกระทบในระดับที่ยังไม่นับสำคัญต่อการดำเนินงานขององค์กร
ความสำคัญปานกลาง	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
ความสำคัญน้อย	ไม่มีผลกระทบใด ๆ ต่อการดำเนินการกิจ

1.4.3. จัดแบ่งลำดับชั้นความลับของข้อมูล

1.4.3.1. ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

1.4.3.2. ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

1.4.3.3. ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

1.4.3.4. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

1.4.4. จัดแบ่งระดับชั้นการเข้าถึง ดังนี้

1.4.4.1. เข้าถึงได้ทุกกลุ่มผู้ใช้งาน ได้แก่ ข้อมูลทั่วไปที่เปิดเผยได้

- 1.4.4.2. เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ ได้แก่ ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ข้อมูลลับ
- 1.4.4.3. เข้าถึงได้เฉพาะผู้มีสิทธิในการบริหารจัดการระบบสารสนเทศ ได้แก่ ข้อมูลระบบ
- 1.4.5. กำหนดช่องทางในการเข้าถึงข้อมูล
 - 1.4.5.1. ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายภายใน ได้ตลอด 24 ชั่วโมง
 - 1.4.5.2. ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเทอร์เน็ตที่อยู่ภายนอก ผ่านระบบ VPN ได้ ตั้งแต่ 6:00-24:00 หรือตามเวลาที่มีการร้องขอและได้รับการอนุมัติแล้วเท่านั้น
 - 1.4.5.2. ผู้ใช้งานเข้าใช้บริการผ่านทางระบบเครือข่ายอินเทอร์เน็ตที่อยู่ภายนอก ได้ตลอด 24 ชั่วโมง หรือตามเวลาที่มีการร้องขอและได้รับการอนุมัติแล้วเท่านั้น
- 1.4.6. กำหนดเวลาและจำนวนระยะเวลาในการเข้าถึงข้อมูล
 - 1.4.6.1. ระบบงานบริการสำหรับผู้ใช้งานทั่วไปเข้าถึงได้ตลอดเวลา ตามที่มีการอนุมัติการเข้าถึง
- 1.5 มีการจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศ โดยจะมีการจัดเก็บข้อมูลการเข้าถึงเป็นล็อกการเข้าใช้งาน เพื่อเป็นหลักฐานในการตรวจสอบ

แนวปฏิบัติการควบคุมการเข้าถึงเครือข่าย

เพื่อควบคุมการให้บริการบนระบบเครือข่ายคอมพิวเตอร์

1. ผู้ดูแลระบบมีการออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ
2. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกบริษัทผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน ก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกบริษัทสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของบริษัท ได้แก่
 - 2.1. การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)
 - 2.2. การพิสูจน์ยืนยันตัวตน ด้วยการใส่รหัสผ่าน (Password)
 - 2.3. การเข้าสู่ระบบสารสนเทศของบริษัท จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง
 - 2.4. การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสข้อมูล ได้แก่ SSL
3. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของบริษัทและเครือข่ายภายนอกกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น
4. ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย ผู้ดูแลระบบมีการจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างบริษัทฯ กับหน่วยงานภายนอก
5. การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่
 - 5.1. ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย
 - 5.2. มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

- 5.3. ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต
6. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบจะมีการกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น
7. ผู้ดูแลระบบมีการกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC Address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง
8. ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่
- 8.1. มีการตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งาน และสอบทานค่าการติดตั้งตามรอบการตรวจสอบ
 - 8.2. มีการควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย
 - 8.3. การขอใช้งานช่องทางการสื่อสารทางอิเล็กทรอนิกส์ (Port-พอร์ต) ดังกล่าวต้องได้รับอนุญาตจากหัวหน้ากลุ่มเทคโนโลยีหรือผ่านช่องทางที่ฝ่ายเทคโนโลยีจัดเตรียมไว้ให้ (พอร์ตที่ฝ่ายเทคโนโลยี กำหนดไว้ เพื่อเป็นการดำเนินการขอข้อมูล จะเป็นมาตรฐานโดยทั่วไปของระบบเทคโนโลยี หรือเพื่อการใช้งานเฉพาะเจาะจง โดยจะไม่กระทบกับการดำเนินการหลัก)
 - 8.4. มีการเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต
9. ผู้ดูแลระบบมีการกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

- 1. การเข้าถึงระบบเครือข่ายไร้สายของหน่วยงานจะต้องมีการบันทึก MAC Address
- 2. ผู้ใช้งานต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
- 3. ผู้ดูแลระบบต้องดำเนินการดังต่อไปนี้
 - 3.1. มีการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
 - 3.2. มีการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
 - 3.3. มีการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
 - 3.4. เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

3.5. เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดายากเพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือเจาะรหัสได้โดยง่าย

3.6. มีการกำหนดค่าใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

3.7. มีการควบคุม MAC Address ชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

3.8. ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

3.9. ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการหรือ หัวหน้ากลุ่มเทคโนโลยี ทราบโดยทันที

แนวปฏิบัติการจัดการการเข้าถึงของผู้ใช้งาน

เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้ และควบคุมการเข้าถึงระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ ให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต

1. กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้

1.1. จัดทำแบบฟอร์มหรือระบบการลงทะเบียนผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

1.2. จัดทำเอกสารแสดงถึงสิทธิที่ต้องการเข้าถึง ที่นอกเหนือจากสิทธิที่ได้รับ และความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

1.3. มีการจัดบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

1.4. กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

1) ต้องเป็นพนักงานบริษัท บุคลากร ของบริษัท หรือบุคคลภายนอกที่มีบัญชีรายชื่อที่ออกโดยฝ่ายเทคโนโลยีและ/หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้ทรัพยากรสารสนเทศของบริษัท และยังไม่สิ้นสุดสถานภาพการพนักงานของบริษัท

2) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูลในส่วนงานนั้นๆ และได้รับมอบหมายจากผู้บังคับบัญชา เช่น การเข้าถึงระบบเว็บไซต์ ที่นอกเหนือจากหน้าที่ปกติที่ได้รับการอนุมัติแล้ว ต้องได้รับการอนุมัติจากหัวหน้าฝ่ายบัญชี

3) ได้รับการอนุมัติจากหัวหน้ากลุ่มเทคโนโลยี หรือผู้ดูแลระบบที่ได้รับมอบหมาย

1.5. กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

- 1) การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน
- 2) การใช้งานที่ขัดต่อข้อกำหนดการใช้งานเครือข่าย
- 3) มีการแจ้งให้มีการเพิกถอนจากหัวหน้าส่วน หรือหัวหน้าหน่วยงานที่เป็นเจ้าของข้อมูล

2. การบริหารจัดการสิทธิของผู้ใช้งาน (Privileges Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะสิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

2.1. มีการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพหรือหน้าที่ความรับผิดชอบ

2.2. มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

2.3. มีการมอบหมายสิทธิและสอดคล้องกับนโยบายควบคุมการเข้าถึง

2.4. มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

3. การบริหารจัดการรหัสผ่าน

3.1. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

3.2. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการเดา

3.3. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

3.4. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

3.5. ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

3.6. มีการจัดการรหัสผ่านของระบบการขายต่างจากการจัดการทั่วไป ตามแนวทางการปฏิบัติ (Work Instruction) ของแต่ละระบบ (Promise, CMPOS, Clexpert) เพื่อความสอดคล้องกับโปรแกรมการขาย และความสะดวกของพนักงานหน้าสาขา โดยจะมีผู้บริหารระดับสูงของแต่ละแบรนด์ เป็นผู้อนุมัติ

4. การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อเปลี่ยนแปลงสถานภาพ

5. ต้องกำหนดหลักสูตร และฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

1. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความสำคัญสูงหรือมีความเสี่ยงสูง การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธียืนยันตัวตนสำหรับระบบสารสนเทศ ดังนี้

1.1. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีภัยคุกคามเดาเดรหัสผ่านจากเครื่องปลายทาง

1.2. มีการกำหนดระยะเวลาสำหรับการป้อนรหัสผ่าน

1.3. จำกัดเข้าถึงระบบปฏิบัติการเฉพาะภายในองค์กร หรืออินทราเน็ต

2. การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบสารสนเทศ ได้แก่

2.1. ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้ชื่อผู้ใช้ (Username) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

2.2. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดจากการใช้ชื่อผู้ใช้ (Username) เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3. การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

3.1. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

3.2. ต้องให้ผู้ใช้งานร้องขอให้ถูกต้องตามกระบวนการ และเก็บรักษาการรหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ ไม่เปิดเผยให้ผู้อื่นทราบ

3.3. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ให้ยากต่อการคาดเดา

3.4. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้นุ้คคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

3.5. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

3.6. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

4. กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้ง เป็นต้น

5. การพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

6. การตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ ผู้ดูแลระบบต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์เมื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อกหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

7. การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบต้องกำหนดให้ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- 7.1. ก่อนใช้งานโปรแกรมยูทิลิตี้ต้องพิสูจน์ตัวตนก่อน
- 7.2. จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- 7.3. ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- 7.4. ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้
- 7.5. โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

8. การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง ผู้บริหารต้องจัดให้ติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

9. การใช้งานระบบเทคโนโลยีสารสนเทศต้องกำหนดให้ตัด และหมดเวลาการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานเกิน 30 นาที

10. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ของผู้ใช้งานไปยังเครื่องปลายทาง เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง ได้แก่ ระบบบัญชีเงินเดือน ระบบฐานข้อมูลบุคคล โดยสามารถเข้าใช้งานระบบในช่วงวันเวลาทำงานของบริษัทในกรณีมีความจำเป็นเร่งด่วนให้ทำการขออนุมัติจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายเพื่ออนุมัติให้เข้าใช้งานระบบเป็นครั้งคราว

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพห้องควบคุมระบบ

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญอันดับต้นๆ ของระบบรักษาความปลอดภัย ความมั่นคงทางกายภาพรวมถึงการป้องกันสถานที่และอุปกรณ์ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม เป็นต้น การป้องกันอุบัติเหตุอันก่อให้เกิดความเสียหายเนื่องจากกระแสไฟฟ้าลัดวงจร อุณหภูมิหรือความชื้น ในห้องควบคุมที่สูงเกินขีดจำกัด หรือการทำการกระทำโดยประมาท เช่น การทำน้ำหยด โดนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ดังนั้นจึงมีความจำเป็นในการป้องกันอาคารและอุปกรณ์โดยกำหนดเป็นนโยบายเพื่อถือปฏิบัติในเรื่องการสร้างห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

1. จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ โดยจัดแบ่งพื้นที่ ดังนี้

1.1. ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

1.2. พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีเซิร์ฟเวอร์ ระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

2. การเข้าไปในพื้นที่ควบคุม

2.1. ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม โดยจะมีการแจ้งความจำนงค์ในการเข้าพื้นที่ก่อน จึงจะสามารถเข้าได้

- 2.2. ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม
- 2.3. ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ควบคุมเว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
- 2.4. ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
- 2.5. บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องมีเจ้าหน้าที่อยู่ด้วยตลอดเวลา
3. การเข้าไปในพื้นที่จำกัดการเข้าถึง
 - 3.1. ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย 1 คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้งและให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง
 - 3.2. ไม่อนุญาตให้บุคคลที่ไม่มีส่วนเกี่ยวข้องเข้า
 - 3.3. ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง
 - 3.4. ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่จำกัดการเข้าถึงเว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
 - 3.5. ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง
 - 3.6. ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย
 - 3.7. ไม่อนุญาตให้ทำการใช้อุปกรณ์ต่อพ่วงโดยตรงเพื่อทำการสำรองข้อมูลออกมา
4. ด้านกายภาพของห้องควบคุมระบบ
 - 4.1. แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น router, switch, server, UPS เป็นต้น
 - 4.2. มี rack ในการจัดเก็บอุปกรณ์ต่างๆที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา
 - 4.3. ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น
 - 4.4. การจัดวางสาย cable network สายไฟฟ้าควรติดป้ายชื่อสายต้นทางปลายทาง และเก็บสายให้เรียบร้อยเพื่อป้องกันการเดินสะดุด
 - 4.5. ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด
 - 4.6. มีระบบรักษาความปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้องโดยระบบ fingerprint scan หรือ RFID เป็นต้น
 - 4.7. มีระบบสังเกตการณ์อุณหภูมิภายใน rack ระบบแจ้งเตือนและป้องกันอัคคีภัย

4.8. มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติ และระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

4.9. มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

4.10. ระบบปรับอากาศแบบควบคุมอุณหภูมิ (50-80°F) และความชื้น (20- 80%)

5. การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

5.1. กรณีติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้แกะหีบห่อและประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุม และพื้นที่จำกัดการเข้าถึงก่อนนำไปติดตั้งเว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

5.2. กรณีที่จำเป็นต้องทำงานก่อสร้าง แก้ไข และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

5.3. ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก 3 เดือน

5.4. มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการด้านเทคโนโลยีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของบริษัทฯ โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา 1 ครั้งต่อปี

1. หน่วยงานภายนอก ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของ

บริษัทฯ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้มีอำนาจสูงสุดของหน่วยงานเจ้าของระบบที่ต้องการเข้าถึง หรือจากผู้บริหารฝ่ายเทคโนโลยี

2. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

2.1. เหตุผลในการขอใช้งาน

2.2. ระยะเวลาในการใช้งาน

2.3. การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

2.4. การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

2.5. การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

3. หน่วยงานภายนอกที่ทำงานให้กับบริษัทฯ ทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของบริษัทฯ โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

4. ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้งปรับปรุงให้ทันสมัย และหากมีการเปลี่ยนแปลงจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

5. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุม

การปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

6. บริษัทมีสิทธิในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

7. ในการจ้างเหมาพัฒนา บำรุงรักษาระบบผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก ได้แก่

7.1. ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่ต้องใช้งาน

7.2. ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

7.3. ต้องบันทึกกิจกรรมการใช้งานข้อมูลเก็บเป็น Log File

7.4. ในระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้น และหน่วยงานที่เกี่ยวข้องกับระบบเห็นชอบ และอนุมัติในการขึ้นระบบก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีตั้งแต่ระดับผู้จัดการขึ้นไป

แนวปฏิบัติการสำรองและการกู้คืนข้อมูล (Procedure and Guide line)

1. การสำรองข้อมูล หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการให้ดำเนินการคัดเลือกและจัดทำระบบสำรองข้อมูล ดังนี้

1.1. ผู้ดูแลระบบงานด้าน Infrastructure มีหน้าที่

1.1.1. ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล

1.1.2. สำรองข้อมูล และ จัดระดับความสำคัญในการสำรองข้อมูล ดังนี้

ระดับ	ความหมาย	คำอธิบายความหมายเพิ่มเติม
0	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินการกิจ
1	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
2	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
3	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินการกิจ
4	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
5	ปิดหน่วยงาน	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

1.1.3. ต้องจัดให้มีการสำรองให้พอเพียง ในระบบที่มีความสำคัญสูง เครื่องที่มีความสำคัญสูงควรเพิ่มความถี่การสำรองให้มากขึ้น ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
1 Web servers	ค่า configure ข้อมูลเผยแพร่บนเว็บไซต์	ก่อนและหลังการเปลี่ยนแปลง ทั้งหมด 1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปนอกพื้นที่สถานที่หรือจัดเก็บที่ระบบคลาวด์อื่น
2 Database	ค่า configure ข้อมูล	ก่อนและหลังการเปลี่ยนแปลง ทั้งหมด 1 ครั้งแรก และนำสื่อบันทึกข้อมูลนั้นไปนอกพื้นที่สถานที่หรือจัดเก็บที่ระบบคลาวด์อื่น และทุกวัน ในส่วนข้อมูลที่เพิ่มเข้ามา
3 Firewall	ค่า configure ข้อมูล Rule ของ Firewall	ก่อนและหลังการเปลี่ยนแปลง จัดเก็บเป็น Base Line ก่อนและหลังการเปลี่ยนแปลง จัดเก็บเป็น Base Line
4 System Server - Active Directory - Windows Update (WSUS)	ค่า configure ข้อมูลในเครื่อง Server	ก่อนและหลังการเปลี่ยนแปลง ทั้งหมด 1 ครั้งแรก และนำสื่อบันทึกข้อมูลนั้นไปนอกพื้นที่สถานที่หรือจัดเก็บที่ระบบคลาวด์อื่น
5 ข้อมูลที่จัดประเภท ความสำคัญของแต่ละ ส่วนงาน	ค่า configure ข้อมูลที่มีความสำคัญมากที่สุด ข้อมูลที่มีความสำคัญปานกลาง	ก่อนและหลังการเปลี่ยนแปลง จัดเก็บทุกวัน และนำสื่อบันทึกข้อมูลนั้นไปนอกพื้นที่สถานที่หรือจัดเก็บที่ระบบคลาวด์อื่น จัดเก็บเป็นรายอาทิตย์ และนำสื่อบันทึกข้อมูลนั้นไปนอกพื้นที่สถานที่หรือจัดเก็บที่ระบบคลาวด์อื่น

ข้อมูลที่มีความสำคัญน้อย

จัดเก็บทุกสองอาทิตย์ และนำสื่อบันทึก

ข้อมูลนั้นไว้นอกพื้นที่สถานที่ หรือ

จัดเก็บที่ระบบคลาวด์อื่น

1.1.4. มีการจัดทำผังหรือขั้นตอนการสำรองข้อมูล

1.1.5. มีการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

1.1.6. มีการจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข

และรายงานต่อผู้บังคับบัญชา

1.1.7. มีการจัดให้มีการสำรองข้อมูลภายนอกสำนักงานในระบบที่มีความสำคัญระดับสูง

1.1.8. มีการจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

1.1.9. มีการดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้

1.1.10. เป็นผู้กำหนดชนิด เช่น Full หรือ Incremental และช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

1.1.11. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

2. การกู้คืนข้อมูล ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์จนเป็นเหตุให้ต้องดำเนินการกู้คืนระบบ ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชา ดังนี้

2.1. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

2.2. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

2.3. สาเหตุและวิธีการกู้คืน

สาเหตุ	วิธีการ
กรณีที่ 1 เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
กรณีที่ 2 เกิดความเสียหายขึ้นกับฐานข้อมูล	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
กรณีที่ 3 เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

กรณีที่ 4 เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
---	--

3. การจัดทำแผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) หน่วยงานที่รับผิดชอบระบบสารสนเทศมีหน้าที่

3.1. ต้องจัดทำแผนความพร้อมกรณีฉุกเฉิน โดยแผนความพร้อมกรณีฉุกเฉินต้องได้รับการเห็นชอบจากประธานบริหารประกอบด้วย

3.1.1. การกำหนดชนิดของภัยพิบัติ

3.1.2. ประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีระดับความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้

3.1.3. กำหนดขั้นตอนรับมือภัยพิบัติ

3.2. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

3.3. ทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินความพร้อมอย่างน้อยปีละ 1 ครั้ง

แนวปฏิบัติในการสำรองข้อมูล

เพื่อป้องกันการเสียหาย และสูญหายของข้อมูลของบริษัทฯ และบริษัทย่อย

การสำรองข้อมูลและระบบสารสนเทศและการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบสารสนเทศสำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษาการปฏิบัติในการสำรองข้อมูลดังนี้

1. พนักงานสารสนเทศทำการสำรองโปรแกรมที่ใช้ปฏิบัติงานเป็นเวอร์ชันที่ระบบการควบคุมเวอร์ชัน (Subversion: SVN) ทำการสำรองทุกครั้งที่มีการปรับเปลี่ยนเวอร์ชัน โดยโปรแกรมที่สำรองมีดังนี้

i. โปรแกรมระบบ Navision

ii. โปรแกรมระบบทรัพยากรบุคคลสำหรับอ่านค่าลายนิ้วมือ Finger Scan

iii. โปรแกรมเว็บการสั่งซื้อสินค้าประเภทของสด (Direct Purchase)

iv. โปรแกรมเว็บการสั่งซื้อสินค้าจากคลังสินค้า (ใบตลาด)

v. โปรแกรมเว็บการเบิกเงินสดย่อย (Petty Cash)

vi. โปรแกรมเว็บ HRGuru (<https://hrguru.zengroup.co.th>)

vii. โปรแกรมเว็บข้อมูลมาตรฐานการปฏิบัติงาน SOP (<https://sop.zengroup.co.th>)

viii. โปรแกรมเว็บข้อมูลลำดับการอนุมัติ (Level of Approve: LOA, <https://loa.zengroup.co.th>)

ix. โปรแกรมเว็บกฎหมาย (<https://legal.zengroup.co.th>)

x. โปรแกรมฐานข้อมูลอื่นๆ ที่ใช้ภายในบริษัทฯ

2. ระบบจะทำการสำรองฐานข้อมูล (Backup Database) โดยอัตโนมัติ ตั้งแต่เวลา 1.00 นาฬิกา โดยฐานข้อมูลที่ทำ การสำรองมีดังนี้

i. ฐานข้อมูลสำหรับระบบ Navision

ii. ฐานข้อมูลสำหรับระบบทรัพยากรบุคคล (HRIS เฉพาะในส่วน HRFocus)

iii. ฐานข้อมูลสำหรับระบบการสั่งซื้อสินค้าประเภทของสด (Direct Purchase)

iv. ฐานข้อมูลสำหรับระบบการสั่งซื้อสินค้าจากคลังสินค้า (ใบตลาด)

v. ฐานข้อมูลสำหรับระบบเว็บการเบิกเงินสดย่อย (Petty Cash)

vi. ฐานข้อมูลสำหรับระบบเว็บ HRGuru (<https://hrguru.zengroup.co.th>)

vii. ฐานข้อมูลสำหรับระบบเว็บกฎหมาย (<https://legal.zengroup.co.th>)

viii. ฐานข้อมูลอื่นที่เกี่ยวข้องกับบริษัท

3. ระบบจะทำการสำรองข้อมูลเว็บไซต์ การตั้งค่าการทำงานระบบ (System Configuration) และฐานข้อมูลเว็บไซต์ (Backup Database) ทุกครั้งที่มีการเปลี่ยนแปลง ณ วันและเวลาที่ทำการเปลี่ยนแปลง โดยเว็บไซต์ที่ทำการสำรองมีดังนี้

i. เว็บไซต์บริษัท (<https://www.zengroup.co.th>)

ii. เว็บไซต์ร้านอาหารญี่ปุ่น Zen (<https://www.zenrestaurant.co.th>)

iii. เว็บไซต์ร้านอาหารญี่ปุ่นอาคะ (<https://www.akayakiniku.com>)

iv. เว็บไซต์ร้านอาหารญี่ปุ่น On The Table (<https://onthetabletokyocafe.com>)

v. เว็บไซต์ร้านอาหารญี่ปุ่น Sushi CYU (<https://onthetabletokyocafe.com>)

4. จัดทำสำเนาการสำรองฐานข้อมูลในข้อ 2 ไปไว้ที่ระบบคลาวด์ ที่อยู่คนละสถานที่ เพื่อป้องกันการเสียหายจากสถานที่ ปัจจุบัน

5. ทำการทดสอบไฟล์ที่ทำการสำรองก่อนขึ้นระบบจริงขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่าง ถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้นจึงต้องมีแนว ปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1. ระบบไฟร์วอลล์

1.1. ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยไตรมาสละครั้ง

1.2. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมี

ดังต่อไปนี้

1.2.1. กลุ่มข้อมูล (Package) ที่ไฟร์วอลล์ได้ปิดกั้น (Block)

1.2.2. ลักษณะของกลุ่มข้อมูล (Package) ที่ถูกปิดกั้น (Block)

- 1.2.3. หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น (Block) เป็นจำนวนมาก
- 1.3. หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา หากไม่สามารถแก้ไขปัญหาได้ให้รายงานต่อผู้อำนวยการหรือผู้บังคับบัญชาสูงสุด
- 1.4. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลกระทบต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที
2. เครื่องคอมพิวเตอร์แม่ข่าย
 - 2.1. ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนเปิดให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้
 - 2.1.1. ติดตั้งไฟร์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เปิดเฉพาะช่องสัญญาณ (port) ที่ใช้งานเท่านั้น
 - 2.1.2. ปิด Service ที่ไม่ได้ใช้งาน
 - 2.1.3. ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง
 - 2.1.4. จำกัดการเข้าถึงจากผู้มีสิทธิสูง เช่น root หรือ Administrator
 - 2.2. หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง
 - 2.3. หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจัดบันทึก ตรวจสอบ แก้ไข และรายงาน เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา
 - 2.4. ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บังคับบัญชา
 - 2.5. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที
3. ภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสเปย์แวร์
 - 3.1. บริษัทฯ ดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน
 - 3.2. หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้เป็นปัจจุบัน อย่างน้อยสัปดาห์ละครั้ง
 - 3.3. ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของซอฟต์แวร์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้
 - 3.3.1. การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมาก
 - 3.3.2. ถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด
 - 3.4. ต้องศึกษาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามี การกระจายภายในเครือข่ายบริษัทฯ
 - 3.5. กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลกระทบต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันทีระดับความรุนแรงของเหตุการณ์



ระดับ ความหมาย คำอธิบายความหมายเพิ่มเติม

- 0 ไม่มีผลกระทบ ไม่มีผลกระทบใด ๆ ต่อการดำเนินงาน
 - 1 กระทบเล็กน้อย มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
 - 2 กระทบค่อนข้างน้อย มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
 - 3 กระทบค่อนข้างรุนแรง มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงาน
 - 4 กระทบรุนแรง มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
 - 5 ปิดหน่วยงาน มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร
4. ประสานงานกับผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยจะมีการเฝ้าระวัง และแจ้งความผิดปกติที่เกิดขึ้นให้กับหน่วยงานเทคโนโลยีสารสนเทศ ซึ่งจะมีการแบ่งระดับความสำคัญในการติดต่อ โดยกรณีที่ต้องติดต่ออย่างเร่งด่วน คือภัยคุกคามที่เป็นอันตรายสูง ส่วนภัยคุกคามอื่นๆ ทางศูนย์เฝ้าระวัง จะทำการจัดทำรายงาน และวิธีการป้องกัน เพื่อทำการปรับปรุงแก้ไขระบบต่อไป

แนวปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

1. เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล
2. กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้ หรือใช้มาตรฐาน DoD 5220.22 M ของ

กระทรวงกลาโหมสหรัฐอเมริกา

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายใหม่ได้	วิธีทำลาย	ระยะเวลาทำลาย
กระดาษ	-	-ใช้การหั่นด้วยเครื่องทำลายเอกสาร	เก็บรักษาไว้ 1 ปี
Flash Drive	ใช้วิธีการ Format	- ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย 1 ปีและตามที่กฎหมายกำหนด
แผ่น CD/DVD		-ใช้การหั่น ดัด เผา ให้สิ้นสภาพการใช้	เก็บรักษาไว้อย่างน้อย 1 ปีและตามที่กฎหมายกำหนด
เทป	ใช้วิธีบันทึกทับ	-ใช้วิธีทุบหรือบดให้เสียหายหรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย 1 ปีและตามที่กฎหมายกำหนด
ฮาร์ดดิสก์	ใช้วิธี Format	-ทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ	เก็บรักษาไว้อย่างน้อย 1 ปีและตามที่กฎหมาย

		-ใช้วิธีการทบทวนทำลายหรือบดให้เสียหาย	กำหนด
พื้นที่จัดเก็บ คลาวด์	ทำการลบข้อมูล และคืนพื้นที่ใน การจัดเก็บ อัตโนมัติ	ทำการลบข้อมูล และติดตามลบที่สำรอง	เก็บรักษาไว้อย่างน้อย 1 ปีและตามที่กฎหมาย กำหนด

การทำลายกรณีนี้ ไม่เกี่ยวข้องกับเรื่อง PDPA ซึ่งกรณีที่เป็น PDPA จะควบคุมตามระเบียบปฏิบัติของ PDPA

แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศและป้องกันการบุกรุกผ่านระบบเครือข่ายจาก
ผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์

1. การจำกัดการเข้าถึงระบบสารสนเทศ

1.1. ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบได้ กำหนดกลุ่ม
ของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูล
จำเป็นต้องใช้งาน

1.2. ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานโปรแกรมประยุกต์หรือ
แอปพลิเคชันและสารสนเทศ โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

1.3. การแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง

1.3.1. การจัดทำบัญชีรายชื่อแยกประเภทโดยแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบ
อินเทอร์เน็ตภายในที่ใช้ภายในบริษัทฯ

1.3.2. ระบบซึ่งมีผลกระทบและมีความสำคัญสูงต่อองค์กร ได้แก่ ระบบสารสนเทศทางการบัญชี
(ERP) ระบบฐานข้อมูลกลางของบริษัทฯ ต้องได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์กร

1.3.3. ระบบซึ่งไวต่อการรบกวน ต้องควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้อง
ปฏิบัติงานแยกเป็นสัดส่วน และกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานใน
ห้องควบคุมดังกล่าวเช่น Payroll

1.3.4. การเข้าถึงระบบสารสนเทศที่มีความสำคัญสูง อนุญาตให้ทำผ่านช่องทางที่กำหนดให้ตามข้อ

2 (การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัทฯ)

1.3.5 บันทึกข้อมูลการใช้งานให้เป็น Log File

2. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัทฯ

2.1. การป้องกันข้อมูลและทรัพย์สินสารสนเทศที่อยู่ในอุปกรณ์สื่อสารประเภทพกพา ผู้ใช้งานต้องมีวิธีป้องกัน
ข้อมูลและทรัพย์สินด้านสารสนเทศในอุปกรณ์สื่อสารประเภทพกพาเมื่อปฏิบัติงานนอกสถานที่ ได้แก่

2.1.1. ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

2.1.2. ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพาเมื่อทิ้งไว้ในที่ไม่มีคนดูแล

2.1.3. ต้องเข้ารหัสข้อมูลที่สำคัญไว้

2.2. การเข้าสู่ระบบระยะไกล (Remote Access) ระบบเครือข่ายของบริษัทฯ ต้องพิสูจน์ตัวตนก่อน
เข้าใช้งาน

2.2.1. การแสดงตัวตน ด้วยชื่อผู้ใช้งาน (Username)

2.2.2. การพิสูจน์ยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

2.2.3. การเข้าสู่ระบบสารสนเทศของบริษัทฯ จากภายใน Network โดยฝ่ายเทคโนโลยี เพื่อการ
support จะต้องร้องขอ รหัสเพื่อเป็นการให้อนุญาต เข้าถึง Desktop ทุกครั้ง

2.2.4. การเข้าสู่ระบบจากระยะไกลต้องใช้การเข้ารหัสข้อมูล ได้แก่ SSL เพื่อเพิ่มความปลอดภัยของ
การรับส่งข้อมูล

2.3. การอนุญาตให้ผู้เข้าใช้ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่เปิดพอร์ตที่
ไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

2.4. การปฏิบัติงานนอกบริษัทฯ ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

3. กระบวนการการร้องขอ การเข้าถึงระบบ

นอกจากระบบพื้นฐาน (ระบบปฏิบัติงาน Windows, Email, ระบบ HRIS เพื่อการจัดการการเข้างาน) แล้วนั้น
กรณีที่พนักงานต้องการเข้าถึงระบบงานอื่นๆ จะต้องทำการร้องขอ เพื่อการอนุมัติการเข้าใช้งานจากหัวหน้างานแต่ละ
ฝ่าย ดังนี้

3. ระบบ Navision มีขั้นตอนปฏิบัติดังนี้

3.1.1 กรณีผู้ใช้งาน อยู่ภายใต้หน่วยงานที่ตำแหน่งชัดเจน ข้อมูลผู้ใช้จะถูกสร้าง และจัดการสิทธิ
การเข้าใช้งานเบื้องต้นอยู่แล้ว ได้แก่ ฝ่ายบัญชี ฝ่ายจัดซื้อ ฝ่ายควบคุมสินค้าคงคลัง

แต่ในกรณี ที่ต้องมีกร้องขอเข้าใช้งานอื่นที่นอกเหนือจากที่ได้รับมอบหมาย ต้องทำแจ้งความ
จำนงค์ผ่านระบบการร้องขอ (Service-F1) หรือแจ้งทางอีเมล โดยผ่านหัวหน้างาน

3.1.2 ระบบจะถูกนำเสนอ นำเสนอหัวหน้าฝ่าย เพื่อการขออนุมัติเข้าใช้งาน

3.1.3. ระบบจะถูกนำเสนอหัวหน้าฝ่ายบัญชี ซึ่งเป็นเจ้าของระบบ (System Owner)

3.1.4 ระบบจะนำเสนอข้อมูลการร้องขอที่ได้รับการอนุมัติแล้ว แจ้งทางฝ่ายบริหารเทคโนโลยี
สารสนเทศ เพื่อดำเนินการตามคำร้อง

* เอกสารการร้องขอ จะถูกจัดเก็บในระบบการร้องขอ (Service-F1) ฝ่ายบริหารข้อมูลเทคโนโลยีสารสนเทศ

3.2. ระบบการขายหน้าสาขา (POS) มีขั้นตอนปฏิบัติดังนี้

3.2.1. ผู้ร้องขอทำการร้องขอผ่านทาง Web Service-F1

3.2.2. ทำการร้องขออนุมัติผ่านทางฝ่ายบุคคล เพื่อยืนยันการเป็นพนักงาน และไม่เป็นผู้
ต้องห้ามในการปฏิบัติงาน

3.2.3. เมื่อฝ่ายบุคคลอนุมัติ ยืนยันตามการร้องขอ ฝ่ายบริหารเทคโนโลยีสารสนเทศ จะ
ดำเนินการตามคำร้อง และจัดส่งข้อมูล Password ให้หัวหน้าพนักงานที่ร้องขอระบบ Service-F1

* กรณีฝ่ายตรวจสอบ จะทำการร้องขอผ่านทางผู้บริหารของแต่ละแบรนด์

3.3. ระบบการร้องขอใช้เงินสดย่อยหน้าสาขา (Petty Cash System) มีขั้นตอนปฏิบัติดังนี้

- 3.3.1. ผู้ร้องขอทำการกรอกแบบฟอร์มการขอเข้าใช้ โดยสามารถ Download ได้ที่เว็บไซต์ <https://HRGuru.zengroup.co.th> ที่เมนู "ดาวน์โหลดแบบฟอร์ม"
- 3.3.2. ระบบการร้องขอจะนำเสนอหัวหน้าฝ่าย เพื่ออนุมัติขั้นตอนการร้องขอ
- 3.3.3. นำแบบฟอร์มที่ได้รับการอนุมัติแล้ว แจ้งทางฝ่ายบริหารเทคโนโลยีสารสนเทศ เพื่อดำเนินการตามคำร้อง
- 3.4. การเข้าถึงไฟล์ข้อมูล (Shared Folder) หรือรายงานต่างๆ (Report)
- 3.4.1. ผู้ร้องขอทำการร้องขอแจ้งผ่านทาง Email
- 3.4.2. ทำการร้องขออนุมัติผ่านทางหัวหน้าฝ่ายต้นสังกัด
- 3.4.3. เมื่อหัวหน้าฝ่ายต้นสังกัด อนุมัติ ยืนยันตามการร้องขอ ฝ่ายบริหารเทคโนโลยีสารสนเทศ จะดำเนินการตามคำร้อง
- 4.ห้องปฏิบัติการ Server
- ไม่อนุญาตให้บุคคลที่ไม่เกี่ยวข้องเข้าห้องปฏิบัติการ Server
 - กรณีที่มีความจำเป็นต้องเข้า ต้องมีการร้องขอและได้รับการอนุมัติจากหัวหน้าฝ่ายเทคโนโลยี
 - หัวหน้างานด้าน Infrastructure เป็นผู้ควบคุมดูแลและนี้ผู้มีสิทธิการเข้าไปดูแลบำรุงเครื่อง Server หรืออุปกรณ์ต่อพ่วง

กรณีที่บุคคลภายนอกต้องเข้าห้องปฏิบัติการ (Server Room) ผู้ร้องขอต้องทำการบันทึกข้อมูลส่วนตัวผู้ร้องขอ คือ ชื่อ-นามสกุล, หน่วยงานต้นสังกัด-ฝ่าย หรือบริษัทของผู้ร้องขอ, เบอร์โทรศัพท์ และหมายเลขประจำตัวบัตรประชาชนให้กับผู้ดูแลระบบและหัวหน้างานทางฝ่ายบริหารเทคโนโลยีสารสนเทศ

b) การเข้าถึงฟังก์ชันงานในส่วนต่างๆ ของระบบ ผู้ดูแลระบบจะทำการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น โดยระบบที่ต้องจัดการสิทธิการเข้าถึงแต่ละฟังก์ชันงานมีดังนี้

i.ระบบ Navision จะแบ่งแยกตามการฝ่ายดังนี้ ฝ่ายบัญชี ฝ่ายการเงิน ฝ่ายบริหารสินค้าคงคลัง ฝ่ายจัดซื้อ ฝ่ายอื่นที่สามารถเข้าใช้งานระบบ Navision นอกเหนือจากที่กล่าวแล้ว จะเป็นการขอเข้าดูรายงานเท่านั้น ซึ่งจะไม่มีการแก้ไข หรือปรับปรุงข้อมูล

ii.ระบบการขายหน้าสาขา (POS) มีประเภทการเข้าถึงข้อมูลคือ

- ระดับพนักงานรับออเดอร์ลูกค้า จะไม่สามารถทำการยกเลิกข้อมูลได้
- ระดับผู้จัดการร้าน จะสามารถยกเลิก (Cancel) การสั่งอาหาร หรือระดับการอนุมัติในระบบการขายที่มีอยู่ในระบบได้

iii.ระบบการร้องขอใช้เงินสดย่อยหน้าสาขา (Petty Cash System) มีประเภทการเข้าถึงข้อมูลดังนี้

- ระดับพนักงานร้องขออนุมัตินำเงินไปใช้ จะทำการร้องขอเท่านั้น
- ระดับผู้อนุมัติ ทำการอนุมัติการร้องขอ
- ระดับผู้ตรวจสอบข้อมูลฝ่ายบัญชี จะทำการเข้าดูข้อมูลเพื่อการตรวจสอบข้อมูลการร้องขอ
- ฝ่ายการเงิน จะทำการปรับตัวเลขข้อมูลการเงินเงินสดกลับไปที่บัญชีของแต่ละสาขาได้

iv. ระบบการสั่งซื้อสินค้าจากคลังสินค้า (ใบตลาด) ประเภทการเข้าถึงข้อมูลคือ

- ฝ่ายดูแลงานสินค้าคงคลัง หรือผู้ดูแลระบบในส่วนของคุณข้อมูลตั้งต้น (Master Data)
- ระดับการสั่งซื้อสินค้า เพื่อสำหรับสาขาทำการสั่งซื้อสินค้า
- ระดับผู้ดูแลหน้าสาขา สามารถดูและแก้ไข ปรับปรุง หรือสั่งซื้อสินค้าเพิ่มให้หน้าสาขาได้

v. ระบบการสั่งซื้อสินค้าประเภทของสด (Direct Purchase) ประเภทการเข้าถึงข้อมูลคือ

- ระดับการสั่งซื้อสินค้า เพื่อสำหรับสาขาทำการสั่งซื้อสินค้า
- ระดับผู้ดูแลหน้าสาขา สามารถดูและแก้ไข ปรับปรุง หรือสั่งซื้อสินค้าเพิ่มให้หน้าสาขาได้

กรณีที่มีการร้องขอเข้าใช้งานในส่วนงานที่ไม่เกี่ยวข้องกัน ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและเจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่

5. การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account)

1. ระบบจะมีการสร้างข้อมูลผู้ใช้งานอัตโนมัติ หลังจากจากระบบการจัดการฝ่ายบุคคลมีการนำเข้าข้อมูลพนักงานที่สมบูรณ์

2. ผู้ดูแล Active Directory จะทำการกำหนดสิทธิ์ของพนักงานที่เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ โดยจะอ้างอิงตามตำแหน่งงานของพนักงาน

3. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด จะทำการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

3.1 มีความเห็นชอบและอนุมัติจากผู้ดูแลระบบงาน

3.2 ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

3.3 ระบบปฏิบัติการ Windows มีกำหนดการเปลี่ยนรหัสผ่านทุก 90 วัน หรือ 3 เดือน

3.4 ระวังการใช้งานทันทีเมื่อพ้นระยะเวลา

4. ระบบจะทำการลบข้อมูลผู้ใช้งานอัตโนมัติ เมื่อมีการปรับปรุงข้อมูลของฝ่ายบุคคล เป็นสิ้นสุดการเป็นพนักงาน หรือพ้นสภาพพนักงาน

5. ในกรณีที่มีความเร่งด่วนในการปรับปรุงข้อมูลพนักงาน ให้ไม่สามารถใช้งานได้ ทางฝ่ายบุคคลจะทำการแจ้งกับหัวหน้าฝ่ายเทคโนโลยี หรือผู้จัดการฝ่ายปฏิบัติการ โดยผ่านการอนุมัติและยืนยันจากหัวหน้างานฝ่ายบุคคลเรียบร้อยแล้ว

แนวปฏิบัติการควบคุมการเข้าถึงจากทางไกล (Remote Access)

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศจากทางไกล โดยมีแนวทางการปฏิบัติ แบ่งเป็น 2 กรณี ดังนี้

1. การควบคุมการเข้าถึงจากทางไกล สำหรับพนักงานในฝ่ายเทคโนโลยีเป็นผู้ใช้งาน

สำหรับการปฏิบัติงานโดยพนักงานฝ่ายเทคโนโลยีเป็นผู้เข้าถึงเครื่องของพนักงานอื่น เพื่อทำการช่วยเหลือการแก้ปัญหาต่างๆ ที่มีความจำเป็นในการที่จะต้องเข้าแก้ไข ซึ่งจะสามารถแก้ไขปัญหาได้ดี และรวดเร็วกว่าการไปที่เครื่อง มีวิธีการดำเนินการดังนี้

- ต้องได้รับการยินยอมและร้องขอจากบุคคลที่มีอำนาจในการครอบครอง หรือปฏิบัติงานอยู่ที่เครื่องที่มีปัญหาเท่านั้น โดยจะมีการแจ้งข้อมูลเครื่องที่ต้องการ และรหัสลับในการการเข้าถึง (Login and Password) จากโปรแกรม TeamViewer หรือการคลิกยอมรับจากกล่องข้อความร้องขอ จากโปรแกรม AnyDesk เท่านั้น
- เมื่อพนักงานฝ่ายเทคโนโลยีได้ทำการแก้ไขปัญหาเรียบร้อยแล้ว พนักงานฝ่ายเทคโนโลยีต้องทำการยกเลิกการเข้าถึง (Log Out) ซึ่ง将无法ทำการปรับปรุงแก้ไขได้

2. การควบคุมการเข้าถึงจากทางไกล สำหรับพนักงานทั่วไปเข้าใช้งานระบบสารสนเทศ

สำหรับพนักงานทั่วไป ที่มีความจำเป็นในการปฏิบัติงานทางไกล ต้องการที่จะเข้าใช้งานข้อมูลสารสนเทศเสมือนกับปฏิบัติงานอยู่ในเครือข่ายหรือเสมือนอยู่ในบริษัท จะต้องดำเนินการดังนี้

- การร้องขอใช้งาน ต้องมีการร้องขอใช้งานก่อน โดยดำเนินการดังนี้
 - ทำการร้องขอ โดยทำการแจ้งเรื่องที่ระบบการร้องขอ Service-F1 โดยทำการกรอกข้อมูลรายละเอียดการร้องขอให้ครบถ้วนตามแบบฟอร์ม
 - ระบบจะนำเสนอหัวหน้าฝ่าย เพื่อขออนุมัติการเข้าใช้งาน
 - ระบบจะส่งแบบฟอร์มที่ได้รับการอนุมัติแล้ว แจ้งทางฝ่ายเทคโนโลยี Infrastructure เพื่อจัดการสร้างข้อมูลการเข้าใช้
 - นำอุปกรณ์ที่ต้องการใช้ปฏิบัติงาน (คอมพิวเตอร์แบบพกพาหรืออุปกรณ์โทรศัพท์) ให้ทางฝ่ายเทคโนโลยีดำเนินการติดตั้งโปรแกรมในการเข้าใช้งานตามคำร้อง
- การปฏิบัติงาน จะดำเนินการได้เมื่อทางฝ่ายเทคโนโลยีสารสนเทศ ส่งข้อมูลการเข้าใช้งานพร้อมการติดตั้งโปรแกรมการเข้าใช้งานเรียบร้อยแล้ว
- การยกเลิก หรือสิ้นสุดการใช้งาน
 - ผู้ร้องขอจะไม่สามารถเข้าใช้งานได้ตามระยะเวลาที่ร้องขอ โดยข้อมูลการเข้าใช้งาน จะไม่สามารถใช้งานได้เพราะมีการถอดถอนสิทธิ์การเข้าใช้งาน
 - ผู้ร้องขอจะไม่สามารถเข้าใช้งานได้ เมื่อผู้ร้องขอสิ้นสภาพการเป็นพนักงานบริษัท หรือมีการแจ้งยกเลิกจากผู้อนุมัติทันที

○ กรณีที่ต้องการใช้งานใหม่ ต้องทำการร้องขอการใช้งานใหม่

การปฏิบัติงานทางไกล ผู้ใช้งานต้องปฏิบัติตามระเบียบวินัยเสมือนปฏิบัติงานอยู่ในบริษัทฯ อย่างเคร่งครัด ต้องไม่ทำการอันใดที่ก่อให้เกิดความเสียหายให้แก่บริษัทฯ เป็นอันขาด

3. การควบคุมการเข้าถึงจากทางไกล สำหรับผู้ให้บริการภายนอกเข้าใช้งานระบบสารสนเทศ

สำหรับผู้ให้บริการภายนอก ที่มีความจำเป็นในการปฏิบัติงานทางไกล ต้องการที่จะเข้าใช้งานข้อมูลสารสนเทศเสมือนกับปฏิบัติงานอยู่ในเครือข่ายหรือเสมือนอยู่ในบริษัทฯ จะต้องดำเนินการดังนี้

- การร้องขอกับหน่วยงานภายในบริษัทที่ประสานอยู่ เพื่อให้หน่วยงานนั้นๆ ร้องขอการเข้าใช้งาน โดยดำเนินการดังนี้
 - ทำการแจ้งหน่วยงานฝ่ายเทคโนโลยี เป็นลายลักษณ์อักษรทาง Email
 - การนำส่ง ต้องนำส่งพร้อมกับหน่วยงานที่เกี่ยวข้องกับงาน เพื่อเป็นการยืนยันความต้องการเข้าใช้งานจริง
 - นำแบบฟอร์มที่ได้รับการอนุมัติและยืนยันจากหน่วยงานที่เกี่ยวข้อง แจ้งทางฝ่ายเทคโนโลยีสารสนเทศ Infrastructure เพื่อจัดการสร้างข้อมูลการเข้าใช้
 - นำอุปกรณ์ที่ต้องการใช้ปฏิบัติงาน (คอมพิวเตอร์แบบพกพาหรืออุปกรณ์โทรศัพท์) ให้ทางฝ่ายเทคโนโลยีดำเนินการติดตั้งโปรแกรมในการเข้าใช้งานตามคำร้อง หรือกรณีไม่สะดวกนำเข้ามาติดตั้ง สามารถประสานงาน Download โปรแกรม และติดตั้งเองได้
- การปฏิบัติงาน จะดำเนินการได้เมื่อทางฝ่ายเทคโนโลยีสารสนเทศ ส่งข้อมูลการเข้าใช้งานพร้อมการติดตั้งโปรแกรมการเข้าใช้งานเรียบร้อยแล้ว
- การยกเลิก หรือสิ้นสุดการใช้งาน
 - ผู้ร้องขอจะไม่สามารถเข้าใช้งานได้ตามระยะเวลาที่ร้องขอ โดยข้อมูลการเข้าใช้งาน จะไม่สามารถใช้งานได้เพราะมีการถอดถอนสิทธิ์การเข้าใช้งาน
 - ผู้ร้องขอจะไม่สามารถเข้าใช้งานได้ เมื่อผู้ร้องขอสิ้นสภาพการเป็นพนักงานบริษัทฯ หรือมีการแจ้งยกเลิกจากผู้อนุมัติทันที
 - กรณีที่ต้องการใช้งานใหม่ ต้องทำการร้องขอการใช้งานใหม่

การปฏิบัติงานทางไกล ผู้ใช้งานต้องปฏิบัติตามระเบียบวินัยเสมือนปฏิบัติงานอยู่ในบริษัทฯ อย่างเคร่งครัด ต้องไม่ทำการอันใดที่ก่อให้เกิดความเสียหายให้แก่บริษัทฯ เป็นอันขาด

ข้อกำหนดการใช้งานเครือข่าย

1. สิทธิการใช้เครือข่าย

1.1. สิทธิการใช้เครือข่ายเป็นสิทธิที่บริษัทฯ มอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิไม่สามารถโอนสิทธิให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

1.2. ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

1.3. ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่

บริษัทฯ กำหนดและตามหลักสากล

2. การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

2.1. การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำการที่ผิดกฎหมาย

2.2. การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจาก

เจ้าของบัญชี

2.3. การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

2.4. การเผยแพร่ข้อมูลของผู้ใช้หรือของหน่วยงานโดยไม่ได้รับอนุญาต

2.5. การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อ

ประสิทธิภาพการทำงานของระบบ

2.6. การพยายามทำลายหรือทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

2.7. การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

2.8. การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์

2.9. การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้อื่น

2.10. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือ

เครือข่ายอื่น

2.11. การเผยแพร่และ/หรือการเข้าถึงสื่อลามกอนาจาร

2.12. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใด ๆ โดยไม่ได้รับอนุญาต

2.13. การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ

2.14. การนำไอพีแอดเดรสของบริษัทไปจดทะเบียนชื่อโดเมนอื่น

2.15. การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบของบริษัทฯ

3. การฝ่าฝืนระเบียบและการพิจารณาโทษ

1.1. บริษัทฯ จะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้และ/หรือบัญชีผู้ใช้

1.2. ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาปรับและ/หรือยกเลิกบัญชีผู้ใช้

1.3. ฝ่ายเทคโนโลยีจะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษแก่ผู้ใช้ที่ฝ่าฝืนระเบียบ

แนวปฏิบัติในการพัฒนาระบบ (Software development methodology)

1. ขั้นตอนกระบวนการพัฒนาระบบ (Software development methodology)

กระบวนการพัฒนาระบบ (Software development methodology) จะเป็นวิธีการ หรือแนวทางการพัฒนาระบบตั้งแต่เริ่มต้น จนเสร็จสิ้นกระบวนการ ตลอดจนการดูแลระบบ เพื่อให้เกิดประโยชน์สูงสุด (System Development life cycle: SDLC)

เพื่อให้เกิดประโยชน์ และตรงตามวัตถุประสงค์ของการพัฒนาระบบ กระบวนการการพัฒนาระบบจึงต้องประกอบด้วยวิธีการต่างๆ ดังนี้

- Process Modeling: เพื่อให้ความเข้าใจการทำงานของระบบงานเดิม ก่อนที่จะนำไปวิเคราะห์ แก้ปัญหา จำเป็นอย่างยิ่ง ที่จะต้องเข้าใจในระบบงานที่เป็นอยู่ก่อน
- Prototyping clarify the user's requirement: การจำลองระบบทำงานที่จะพัฒนา ศึกษาความเป็นไปได้ ตามความต้องการของผู้ใช้ เพื่อให้เข้าใจตรงกัน ก่อนจะลงมือพัฒนา
- The scope of responsibility is clearly: ความเข้าใจตรงกัน ระหว่างผู้พัฒนา และผู้ใช้ โดยอยู่บนพื้นฐาน การใช้งานจริง และความเป็นไปได้ในการพัฒนา
- กระบวนการพัฒนา วางแผน เทคนิคการนำมาใช้พัฒนา การทดสอบหรือตรวจสอบการทำงานของระบบ ตลอดจนการดูแลรักษาระบบ
- เอกสารที่เกี่ยวข้องในการพัฒนาระบบ เพื่อใช้เป็นคู่มือ
- ขั้นตอนที่เป็นลำดับตั้งแต่ต้นจนเสร็จเรียบร้อย เป็นระบบที่ใช้งานได้ ซึ่งนักวิเคราะห์ระบบต้องทำความเข้าใจให้ดีว่าในแต่ละขั้นตอนจะต้องทำอะไร และทำอะไร

ขั้นตอนการพัฒนาระบบมีอยู่ด้วยกัน 5 ขั้นตอนใหญ่ๆ ด้วยกัน คือ

1) ขั้นตอนการรวบรวมความต้องการ (Requirement Analysis/System Analysis)

การทำความเข้าใจกับปัญหา และความต้องการของผู้ใช้ ซึ่งรวมไปถึงการจัดส่งงานตามแผนการดำเนินงาน โดยผู้ร้องขอและทีมพัฒนาจะต้องเข้าใจตรงกันตามความต้องการของระบบทั้งหมด เพื่อจะได้เป็นแนวทางของการพัฒนาระบบทั้งหมด จะมีขั้นตอนที่เป็นองค์ประกอบอย่างน้อยคือ

- Examine current system ตัวอย่างการทำงานปัจจุบัน และความต้องการ
- นิยาม ความหมาย คำจำกัดความต่างๆ เพื่อความเข้าใจที่ตรงกัน
- Conceptual data model ความหมายรูปแบบ หรือรูปภาพ นิยามข้อมูล ที่เป็นลักษณะเฉพาะเข้าใจตรงกัน
- Build conceptual process model รูปแบบ หรือแผนผังการทำงาน ที่เข้าใจโดยง่าย
- การจัดการความปลอดภัยพื้นฐาน ที่กำหนดและออกแบบพร้อมกับบริษัท เช่น การจัดการปริมาณข้อมูล การออกแบบการเดินทางของข้อมูล ที่ต้องรองรับกับระบบพื้นฐานของบริษัท และมีความปลอดภัย (Secure)

2) ขั้นตอนการออกแบบเบื้องต้น (High Level Design)

การออกแบบระบบในส่วนของการทำงานหลัก มีองค์ประกอบอย่างน้อยดังนี้

- การจัดทำรูปแบบการทำงานของระบบคร่าวๆ เช่น โครงสร้าง Web Site(Prototype)
- รูปแบบโครงสร้างอุปกรณ์ที่จะใช้ให้ระบบทำงาน เช่น Computer Server, Network
- รูปแบบการทำงานของแต่ละส่วนงานของผู้ใช้

3) ขั้นตอนการออกแบบเชิงลึก (Low Level Design)

ในกรณีที่ให้บริการพัฒนาระบบภายนอก (Outsourcing) ต้องมีการออกแบบระบบ ในแต่ละส่วนโดยละเอียด เพื่อให้ทีมพัฒนาระบบภายนอก และพนักงานสารสนเทศเข้าใจได้ตรงตามความต้องการ มีองค์ประกอบอย่างน้อยดังนี้

- การจัดทำตัวอย่างหน้าจอของ Web Page โดยอธิบายความสัมพันธ์ของข้อมูลให้ตรงกัน ในรูปแบบที่เข้าใจง่าย เช่นรูปภาพ
- การพัฒนาโครงสร้างข้อมูลเชิงสัมพันธ์ (Database)
- รูปแบบการทำงานของแต่ละส่วนงานของผู้ใช้

4) ขั้นตอนการพัฒนา (Construction)

การพัฒนาระบบ จากการออกแบบทั้งหมด โดยจะรวมไปถึงการทดสอบเบื้องต้นของแต่ละส่วนของการทำงานทั้งระบบ การดำเนินการจะพัฒนาที่ระบบที่จัดเตรียมไว้สำหรับการพัฒนา (Development Environment)

5) ขั้นตอนการทดสอบ (Testing)

การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบและการดำเนินงานของระบบ หลังจากที่มีการพัฒนาทั้งหมดเสร็จเรียบร้อยแล้ว โดยแบ่งเป็นแต่ละส่วนตามการพิจารณาตามข้อตกลงร่วมกันกับทางผู้ร้องขอ ผู้พัฒนา ดังนี้:

5.1) Unit Testing การทดสอบเบื้องต้น โดยแยกเป็นการทำงานของแต่ละส่วน โดยการทดสอบในขั้นตอนนี้ จะเป็นของทีมพัฒนาระบบหลังจากที่มีการพัฒนาแล้ว หรือขณะที่พัฒนา เช่น การทดสอบหน้าจอการสร้างข้อมูล จะทำการทดสอบข้อมูลรายละเอียดของแต่ละส่วน ว่าสามารถบันทึก ตรวจสอบความถูกต้องได้ การดำเนินการจะพัฒนาที่ระบบที่จัดเตรียมไว้สำหรับการพัฒนา (Development Environment)

5.2) Integration and System Testing (SIT) การทดสอบการทำงานกรณีที่มีส่วนการทำงานติดต่อนำเข้าหรือส่งออกจากระบบอื่น เช่น มีการนำเข้าข้อมูลที่มาจากร Microsoft Excel เป็นต้น โดยจะมีการทำงานได้อย่างถูกต้องทั้งกระบวนการตั้งแต่ต้น จนถึงกระบวนการ ในกรณีที่การทำงานผิดพลาดในขั้นตอนนี้จะทำการแก้ไขใหม่และทำการทดสอบตั้งแต่ขั้นตอนการทดสอบ Unit Test

การดำเนินการจะพัฒนาที่ระบบที่จัดเตรียมไว้สำหรับการพัฒนา (Development Environment)

5.3) Environment Setup เป็นขั้นตอนการจัดเตรียมเครื่องคอมพิวเตอร์ให้เหมือนการปฏิบัติงานจริง เพื่อจะทำการทดสอบการปฏิบัติงานเสมือนจริงของระบบต่อไป

5.4) User Acceptance testing (UAT) การทดสอบการทำงานของระบบ โดยผู้ใช้งาน หรือเพื่อให้ผู้ใช้งาน ได้เห็นว่า การปฏิบัติงานของระบบนั้น สามารถปฏิบัติงานได้ตรงตามความต้องการจริงหรือข้อมูลจำลองมาจากข้อมูลจริง โดยการทดสอบในขั้นตอนนี้ จะได้รับการยืนยันความถูกต้องทุกขั้นตอนการทำงานจากผู้ใช้งาน การดำเนินการจะพัฒนาที่ระบบที่จัดเตรียมไว้สำหรับการทดสอบ (Test Environment)

6) ขั้นตอนสอนการใช้งาน (Training)

หลังจากขั้นตอนการทดสอบและแก้ไขดำเนินการเรียบร้อยแล้ว พนักงานฝ่ายเทคโนโลยีสารสนเทศหรือนักพัฒนาระบบจะทำการนำระบบที่พร้อมใช้งานติดตั้งที่ระบบการสอนการใช้งาน (Training Environment) ในขั้นตอนนี้ ผู้ใช้งานจะได้รับคู่มือการใช้งานโปรแกรม และได้รับการสอนการใช้งานแยก

7) ขั้นตอนการใช้งานและการดูแลรักษา (Warranty and Maintenance)

พนักงานระบบสารสนเทศจะทำการติดตั้ง และตั้งค่าระบบที่ชุดอุปกรณ์ที่ใช้ปฏิบัติงานจริง (Production Environment) เพื่อให้ระบบพร้อมใช้งาน ณ วันที่ได้กำหนดการเริ่มใช้ ทางผู้พัฒนาระบบจะดูแลและแก้ไขส่วนการใช้งานที่พบปัญหา (Warranty) ที่ไม่พบจากการทดสอบ โดยการจัดการในส่วนนี้ อาจจะมีการปรับปรุง หรือเปลี่ยนแปลงการทำงานได้ แต่จะไม่กระทบกับรูปแบบการทำงานที่ได้ตกลงร่วมกันไว้ในช่วงของการออกแบบ (Requirement & Analyst) ที่ได้ตกลงกัน ฝ่ายเทคโนโลยีสารสนเทศจะติดตามผลการทำงาน คอยประสานงานให้ความสะดวกกับผู้ใช้งาน

การดำเนินการขั้นตอนที่ต้องมีการอนุมัติ เพื่อเป็นการยืนยันความเข้าใจ ความถูกต้องของแต่ละขั้นตอน ตลอดจนผลการดำเนินงาน คือ

- | | | |
|---------------------------------|---|---|
| • ขั้นตอนการรวบรวมความต้องการ | ยืนยันความถูกต้องของความต้องการ กระบวนการ | อนุมัติโดย
หัวหน้าฝ่ายที่ร้องขอ
ฝ่ายกำกับกิจการฯ
หัวหน้าฝ่ายเทคโนโลยีและผู้จัดการที่เกี่ยวข้อง |
| • ขั้นตอนการออกแบบ | เพื่อยืนยันความถูกต้อง | อนุมัติโดย
หัวหน้าฝ่ายที่ร้องขอ หรือผู้แทน
หัวหน้าฝ่ายเทคโนโลยี/ผู้จัดการฝ่าย |
| • ขั้นตอนที่อยู่ระหว่างการพัฒนา | จะเป็นการรายงานความคืบหน้า | รับทราบโดย
หัวหน้าฝ่ายที่ร้องขอ หรือผู้แทน
หัวหน้าฝ่ายเทคโนโลยี/ผู้จัดการฝ่าย |

- | | | |
|--|---------------------------|--|
| ● ขั้นตอนการทดสอบ | เพื่อยืนยันผลการดำเนินงาน | รับทราบโดย
หัวหน้าฝ่ายที่ร้องขอ
ฝ่ายกำกับกิจการฯ
หัวหน้าฝ่ายเทคโนโลยี |
| ● ขั้นตอนการนำระบบที่
ดำเนินการเรียบร้อยแล้ว เข้าสู่
เครื่องจริง | เพื่อรับทราบ | รับทราบและอนุมัติการใช้โดย
หัวหน้าฝ่ายที่ร้องขอ
ฝ่ายกำกับกิจการฯ
หัวหน้าฝ่ายเทคโนโลยี |

ผู้พัฒนาโปรแกรม หรือหน่วยงานที่สนับสนุนการทำงานของโปรแกรม ต้องมีส่วนช่วยในการนำข้อมูลที่ไม่ใช้แล้วออกจากระบบ (Archive) เพื่อเป็นการช่วยให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ และไม่ขัดต่อกฎหมาย รวมถึงการปรับปรุงระบบในกรณีที่มีการติดต่อกับระบบอื่น แล้วต้องมีการเปลี่ยนแปลง หรือ Upgrade ให้รองรับการทำงาน

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change control procedures)
การเปลี่ยนแปลงระบบ การพัฒนาระบบมีการควบคุม โดยปฏิบัติตามขั้นตอนคร่าวๆ ดังนี้

- รับข้อมูลการร้องขอจากฝ่ายที่ต้องการปรับเปลี่ยน รวมทั้งการปรึกษาร่วมกัน ในการหาวิธีการและผลลัพธ์เดียวกัน วิเคราะห์ผลดีในการปรับเปลี่ยน ว่ามีความจำเป็น หรือคุ้มค่ากับการปรับเปลี่ยนมากน้อยเพียงใด
- จัดทำเอกสารอ้างอิงการปรับเปลี่ยน วิเคราะห์ และประเมินขั้นตอนการจัดทำ และระยะเวลา เพื่อยืนยันกับฝ่ายที่ร้องขอ และอนุมัติกับหัวหน้าส่วนที่เกี่ยวข้อง รวมทั้งฝ่ายกำกับดูแลกิจการที่ดี ก่อนการดำเนินการ
- ดำเนินการจัดทำตามที่ได้ตกลงร่วมกัน
- ติดตามผลการดำเนินการ ตั้งแต่เริ่มกระบวนการปรับเปลี่ยนในแต่ละขั้นตอน ให้มีการรายงานผลเป็นระยะ และสรุปผลการดำเนินการ

ข้อกำหนดการใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

จดหมายอิเล็กทรอนิกส์ (e-mail) เป็นบริการที่บริษัทฯ จัดให้พนักงานใช้เพื่อความคล่องตัว รวดเร็ว ในการสื่อสารประสานงานระหว่างบุคคล กลุ่มงาน ทั้งภายในและภายนอกบริษัท ภายใต้ชื่อโดเมน zengroup.co.th ในการใช้จดหมายอิเล็กทรอนิกส์ ผู้ใช้มีหน้าที่พึงปฏิบัติดังต่อไปนี้

1. ข้อกำหนดในการใช้

1.1 ผู้ใช้มีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะตัวและไม่อนุญาตให้ผู้อื่น เข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

1.2. ผู้ใช้ที่พบว่าไม่มีสิทธิที่จะถามหรือร้องขอให้ผู้อื่นเปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

1.3. ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม เว้นแต่ได้รับการมอบหมายจากผู้บังคับบัญชาสูงสุดตามสายงานของเจ้าของบัญชีและรองประธานเจ้าหน้าที่บริหารกลุ่มทรัพยากรบุคคล

1.4. การใช้จดหมายอิเล็กทรอนิกส์ในลักษณะต่อไปนี้เป็นสิ่งต้องห้ามดังนี้

- (1) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น
- (2) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่
- (3) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับของบริษัท
- (4) การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นๆ ส่งมาจากบุคคลอื่น
- (5) การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง
- (6) การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย เช่น เส้นทาง วันเวลาการส่ง
- (7) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล
- (8) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่ดูหมิ่นเหยียดหยาม หรือแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ
- (9) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วิดีโอ เสียง ที่มีลักษณะหมิ่นประมาทหรือลามกอนาจาร
- (10) การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรมหรืองาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์
- (11) การส่งจดหมายอิเล็กทรอนิกส์ กระจ่ายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร
- (12) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบต่อระบบจดหมายอิเล็กทรอนิกส์ หรือเครือข่ายลดทอนประสิทธิภาพลง
- (13) การส่งจดหมายอิเล็กทรอนิกส์ กระจ่ายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

ผู้ใช้ใดที่จงใจฝ่าฝืนจะถูกลงโทษตามระเบียบ-ข้อบังคับบริษัท

2. โควตาบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์ ของผู้ใช้แต่ละรายจะมีโควตากำหนดการใช้งานดังนี้

- 2.1. ขนาดข้อมูลรวมที่เก็บในเซิร์ฟเวอร์ต่อผู้ใช้ 100 GB ต่อบัญชีผู้ใช้
- 2.2. ขนาดของไฟล์แนบต่อการส่งจดหมายอิเล็กทรอนิกส์ หนึ่งฉบับ ไม่เกิน 150 MB แต่ระบบจะมีการแจ้งเตือนในกรณีที่มีไฟล์ใหญ่ ซึ่งไม่แนะนำให้มีการจัดส่งไฟล์ใหญ่ ผู้ใช้งานสมควรทำการแชร์ไฟล์ให้เป็นการ Download แทน

- 2.3. อัตราส่งจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด 10,000 จดหมายต่อ วัน และ 500 ผู้รับต่อการส่งแต่ละครั้ง
- 2.4. จำนวนจดหมายอิเล็กทรอนิกส์ ต่อวันเวลาที่กำหนด 30 จดหมายต่อ การส่งภายใน 1 นาที
- 2.5. โควตาเหล่านี้อาจแตกต่างกันตามประเภทและภารกิจของผู้ใช้ การกำหนดโควตาให้อยู่ในดุลยพินิจของฝ่ายเทคโนโลยี โดยสามารถเพิ่มหรือลดค่าแต่ละบัญชีจดหมายอิเล็กทรอนิกส์ตามความเหมาะสมเพื่อให้การใช้งาน และการบริหารจัดการเป็นไปอย่างมีประสิทธิภาพ
3. การตรวจระบบ ฝ่ายเทคโนโลยีมีนโยบายปกป้องข้อมูลส่วนบุคคลและให้ใช้จดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนภารกิจของบริษัท โดยไม่ตรวจดูจดหมายอิเล็กทรอนิกส์ที่รับส่งตามปกติ แต่ฝ่ายเทคโนโลยี มีการระบุพันตามกฎหมายที่ต้องติดตั้งระบบบันทึกข้อมูลจราจรและการเฝ้าระวังเพื่อคงไว้ซึ่งบริการที่มั่นคงปลอดภัยและมีประสิทธิภาพ ฝ่ายเทคโนโลยีบริษัทฯ สงวนสิทธิในการใช้ระบบเฝ้าระวังเพื่อตรวจเนื้อหาจดหมายอิเล็กทรอนิกส์ที่เป็นภัยต่อระบบคอมพิวเตอร์และกลั่นกรองหรือระงับการเผยแพร่โดยอัตโนมัติ ตลอดจนสงวนสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์เพื่อสืบสวน สอบสวน เมื่อระบบเฝ้าระวังแจ้งเตือนถึงปัญหาด้านความมั่นคงปลอดภัยจากการใช้จดหมายอิเล็กทรอนิกส์ใดๆ หรือการร้องขอจากเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือ ตามกฎหมายอื่นที่เกี่ยวข้อง
5. การระงับบัญชีจดหมายอิเล็กทรอนิกส์ บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่ให้อำนาจให้ผู้ดูแล ซึ่งผู้ดูแลไม่สามารถโอนสิทธิให้แก่ผู้อื่นใช้ได้ ฝ่ายเทคโนโลยีของบริษัทฯ คงไว้ซึ่งอำนาจในการจำกัดระงับ หรือเพิกถอนสิทธิให้แก่ผู้ใดโดยไม่ต้องแจ้งให้ผู้ใดทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์
6. เมื่อผู้ดูแลพบสภาพการเป็นพนักงานของบริษัทฯ สามารถระงับบัญชีผู้ใช้ ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ผ่านบัญชีนั้นถูกระงับไปด้วย
7. บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้บังคับบัญชาสูงสุดตามสายงานร่วมฝ่ายบุคคลหากพบว่ามีผู้ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้โดยยื่นคำร้องเป็นลายลักษณ์อักษรที่ฝ่ายเทคโนโลยี
8. บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยทันทีโดยหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบต่อประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้นั้นหรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ ฝ่ายเทคโนโลยีมีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใดทราบล่วงหน้า หากพิสูจน์ได้ว่ามีความจงใจจะมีโทษตามระเบียบข้อบังคับบริษัทฯ
9. กรณีที่ลืม Password ในการเข้าใช้ จดหมายอิเล็กทรอนิกส์ จะต้องร้องขอผ่านช่องทางระบบ Service- F1 ให้แก้ไข Password ที่ฝ่ายเทคโนโลยี ในกรณีที่ไม่สามารถแสดงตนได้ที่ฝ่ายเทคโนโลยี Password จะถูกส่งให้กับผู้ใช้งานโดยตรง และในกรณีที่ เป็น Email สาขา ข้อมูล Password จะถูกส่งให้กับ Area manager ที่ได้มีการร้องขอเข้ามา

แนวปฏิบัติการสร้างความตระหนักเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เนื่องจากการปฏิบัติงานในยุคปัจจุบัน มีการเปลี่ยนแปลงด้านเทคโนโลยีรวดเร็ว และหลากหลาย ซึ่งมีความจำเป็นที่จะต้องปฏิบัติให้เหมาะสม ไม่ผิดต่อแนวทางการปฏิบัติงานของบริษัท และกฎหมาย ผู้ปฏิบัติงาน สมควรเป็นอย่างยิ่ง ที่ต้องพึงระวัง และตระหนักถึงความมั่นคงปลอดภัยทางด้านเทคโนโลยี ที่จะส่งผลกระทบกับการปฏิบัติงานของตนเองและบริษัท

บริษัทฯ จึงได้จัดตั้งหน่วยงานฝ่ายเทคโนโลยี เป็นศูนย์กลางคอยควบคุม ช่วยกำกับดูแล และคอยให้คำปรึกษา และประสานงานเรื่องเกี่ยวกับระบบเทคโนโลยีกับหน่วยงานอื่นที่เกี่ยวข้อง อาทิเช่น

ฝ่ายกำกับดูแลกิจการที่ดี – คอยให้คำปรึกษากฎระเบียบ ความถูกต้องในการดำเนินกิจการ

ฝ่ายการตลาดดิจิทัล – ประสานงานเกี่ยวกับระบบงานข้อมูลลูกค้า

ฝ่ายบัญชี และการเงิน – ดูแลให้คำปรึกษาด้านระบบบัญชี

ฝ่ายควบคุมสินค้าคงคลัง – ดูแลให้คำปรึกษาด้านระบบสินค้าคงคลัง การส่งสินค้า เป็นต้น

ทั้งนี้ เพื่อคอยสนับสนุนงานของแต่ละส่วน ให้มีความมั่นคงปลอดภัย และเรียบร้อย

โดยฝ่ายเทคโนโลยี จะมีการสนับสนุนให้บริการ ประสานงานการรักษาความมั่นคงปลอดภัย ออกเป็น แต่ละด้านดังนี้

- 1.) ด้านการสนับสนุนและประสานงาน คอยช่วยเหลือผู้ใช้งานทั่วไป ทั้งภายใน เช่นพนักงานภายในบริษัท หรือสาขา และภายนอกองค์กร เช่น ลูกค้าเฟรนไชส์ คู่ค้า เป็นต้น โดยจะจัดสรร เตรียมความพร้อมด้านทรัพยากรเทคโนโลยี พร้อมทั้งให้คำปรึกษาความเหมาะสมในการนำระบบเข้ามาปรับใช้

โดยสามารถเข้ามาปรึกษากับหน่วยงานเทคโนโลยีตามช่องทางที่ให้บริการ คือ Email โทรศัพท์ ช่องทางไลน์ (Line) หรือแม้แต่การเข้ารับการบริการที่หน่วยงาน

- 2.) ด้านเฝ้าระวังภัยคุกคามทางไซเบอร์ เป็นศูนย์การรักษาความมั่นคงปลอดภัยดำเนินการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ให้แก่บริษัท ดังนี้

- a) เฝ้าระวังความเสี่ยงและติดตามแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ รวมถึงดำเนินการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อดำเนินการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที
- b) วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้บริษัท สามารถดำเนินการมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่พนักงาน ในการตรวจจับ หรือป้องกันเหตุการณ์ที่อาจนำมาสู่การบุกรุก และการวิเคราะห์ข้อมูลเบื้องต้น เป็นต้น

- c) เพื่อประโยชน์ในการเฝ้าระวังและแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้แต่ละหน่วยงานภายใน ให้มีการรับลงทะเบียนข้อมูลและจัดทำรายงานปัญหา นำไปเป็นข้อมูลในการป้องกันภัยคุกคาม เป็นลำดับต่อไป
 - d) จัดทำรายละเอียดโครงสร้างพื้นฐานสำคัญทางข้อมูลสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ ที่ใช้ในการดำเนินภารกิจหรือให้บริการในกิจการ ซึ่งจำเป็นต้องมีการเฝ้าระวัง หรือดำเนินการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ และปรับปรุงข้อมูลดังกล่าว ให้เป็นปัจจุบันอยู่เสมอ
- 3.) ด้านการรับมือภัยคุกคามด้านไซเบอร์ เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริษัท ดังต่อไปนี้
- a) เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนให้การสนับสนุนข้อมูลต่างๆ ที่จำเป็นต่อหน่วยงาน เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะ หรือช่องทางอื่นใดตามที่ฝ่ายกำกับฯ กำหนด
 - b) ให้การช่วยเหลือ แนะนำ หรือสนับสนุนหน่วยงาน ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และปฏิบัติงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแลในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์
 - c) เมื่อศูนย์เฝ้าระวังความมั่นคงปลอดภัยระบบคอมพิวเตอร์มีการแจ้งการเปลี่ยนแปลงระดับ หรือยกระดับการแจ้งเตือน หรือพบการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์หรือผลกระทบต่อการกิจ ฝ่ายเทคโนโลยีจะดำเนินการแจ้งเตือนไปยังหน่วยงานต่างๆ เพื่อให้เตรียมความพร้อมในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์
 - d) ในการดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ฝ่ายเทคโนโลยีจะคอยให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแล ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และแนวปฏิบัติขององค์กร ให้ดำเนินมาตรการให้มีคุณภาพ
- 4.) ด้านการดำเนินมาตรการด้านการบริหาร จัดการคุณภาพที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และผู้ใช้งาน เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่องค์กร ที่อยู่ภายใต้การดูแล โดยมีหน้าที่และความรับผิดชอบดังต่อไปนี้
- a) ผลักดันและสนับสนุนการสร้างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

- b) ผลักดันและสนับสนุนการเพิ่มความรู้ความสามารถของแต่ละหน่วยงาน เพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางด้านข้อมูลสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ
- c) ฝ่ายเทคโนโลยี ดำเนินการจัดให้มีการฝึกอบรมและให้ความรู้แก่หน่วยงาน เพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Education Training and Awareness หรือ “ETA”) เช่น การวางแผนรับมือในสถานการณ์ที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์หรือการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น โดยประสานงานกับฝ่ายการฝึกอบรม ให้มีการกำหนดเป็นหลักสูตรบังคับให้กับพนักงาน ในการเรียนรู้เบื้องต้นอย่างน้อย ปีละ 1 ครั้ง
- d) ฝ่ายเทคโนโลยี มีการฝึกอบรมความสามารถด้านเทคนิคที่เป็นมาตรฐานในการดูแลรักษาความมั่นคงปลอดภัยด้านไซเบอร์ในด้านต่างๆ เพื่อนำมาปรับปรุงองค์กร ให้มีประสิทธิภาพมากขึ้น และเป็นปัจจุบัน
- e) ดำเนินการแจ้งข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย ให้กับองค์กรเป็นระยะ เพื่อสร้างความตระหนักถึงภัยด้านไซเบอร์ ที่จะทำให้เกิดผลกระทบ ทั้งทางตรง และทางอ้อม
- g) ผลักดันให้มีการประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกัน หรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการร้องขอ โดยดำเนินการตรวจสอบความมั่นคงปลอดภัย (security assessments) ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ด้วยวิธีการต่าง ๆ และให้คำแนะนำเพื่อยกระดับคุณภาพของการดำเนินมาตรการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีความแข็งแกร่งมากขึ้น

นโยบายหรือหลักเกณฑ์ใดที่มีมาก่อนหน้านี้และขัดแย้งกับนโยบายฉบับนี้ ให้ยกเลิกและให้ถือตามนโยบายฉบับนี้

นโยบายฯ ฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ ๑ พฤษภาคม พ.ศ. ๒๕๖๗ เป็นต้นไป

(นายสรกรณท์ จิราวิวัฒน์)

ประธานเจ้าหน้าที่บริหาร