ประกาศที่ 10/2564
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
บริษัท สกาย ไอซีที จำกัด (มหาชน)

วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท สกาย ไอซีที จำกัด (มหาชน) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยในหลากหลายรูปแบบที่มีผลต่อการดำเนินการทางธุรกิจและลดความเสี่ยงที่มีแนวโน้มว่าจะเกิดขึ้น โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

นโยบาย

1. เพื่อป้องกันภัยคุกคามและความเสี่ยงต่าง ๆ ที่มีผลต่อธุรกิจของบริษัท ซึ่งอาจจะเกิดขึ้นโดยตั้งใจหรือไม่ตั้งใจ ทั้งจากภายในและภายนอกองค์กร คณะกรรมการและผู้บริหารของบริษัท สกาย ไอซีที จำกัด (มหาชน) จึงเล็งเห็นความสำคัญนี้พร้อมอนุมัติให้มีการใช้นโยบายความปลอดภัยข้อมูลฉบับนี้ โดยเป็นไปตามกฎเกณฑ์ ข้อบังคับที่มีการประกาศใช้ในประเทศไทย
2. นโยบายฉบับนี้ครอบคลุมในเรื่องดังต่อไปนี้
   - 2.1 ข้อมูลของบริษัทจะต้องได้รับการปกป้องกันจากผู้**ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล**[1]นั้น ๆ ข้อมูลจำเป็นต้องถือเป็นความลับของบริษัท นอกจากนี้ข้อมูลยังต้องถูกเก็บรักษาให้ครบถ้วนสมบูรณ์ ไม่มีการเปลี่ยนแปลงจากเดิมโดยไม่ได้รับอนุญาต หรือจากบุคคลที่ไม่มีสิทธิ์ในการแก้ไขเปลี่ยนแปลงข้อมูลนั้น ๆ และที่สำคัญข้อมูลนั้นจำเป็นต้อง**สามารถนำมาใช้งานได้**เมื่อจำเป็นต้องนำมาใช้ในการทำงาน
   - 2.2 **หน้าที่ความรับผิดชอบ**ของข้อมูลนั้นจำเป็นต้องมีผู้ดูแลและรับผิดชอบอย่างชัดเจน
   - 2.3 **การควบคุมการเข้าถึง**ข้อมูลนั้นจำเป็นต้องมีผู้ดูแลและรับผิดชอบอย่างชัดเจน
   - 2.4 จำเป็นต้องมีการวางแผนสำรองเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง และต้องมีการปรับปรุงดูแลแผนนั้นให้ทันต่อเหตุการณ์เสมอ พร้อมทั้งต้องมีการทดสอบแผน[2] ภายใต้แผนฉุกเฉินของแผนกเทคโนโลยีสารสนเทศ
   - 2.5 **การอบรมเกี่ยวกับความปลอดภัยของข้อมูล**สำหรับพนักงานทุกคนในองค์กร
   - 2.6 **การพบเจอเหตุการณ์จริงหรือข้อสงสัยเกี่ยวกับช่องโหว่ของความปลอดภัยของข้อมูล**จำเป็นต้องรายงานหน่วยงานความปลอดภัยข้อมูล เพื่อทำการตรวจสอบอย่างละเอียด

[1] ข้อมูลมีอยู่ในหลากหลายรูปแบบ ซึ่งรวมถึงข้อมูลที่ถูกเก็บอยู่ในคอมพิวเตอร์ ข้อมูลที่ถูกส่งผ่านระบบเครือข่าย ข้อมูลที่ทำการพิมพ์ออกมาหรือเขียนลงกระดาษ ข้อมูลที่ใช้ส่งผ่านแฟกซ์ หรือเก็บอยู่ในแผ่นดิสก์หรือเทป แม้กระทั่งข้อมูลที่เป็นการคุยระหว่างโทรศัพท์

[2] แผนนี้จะทำให้พนักงานสามารถเข้าถึงข้อมูลและระบบที่จำเป็นต้องใช้ในการทำงานได้

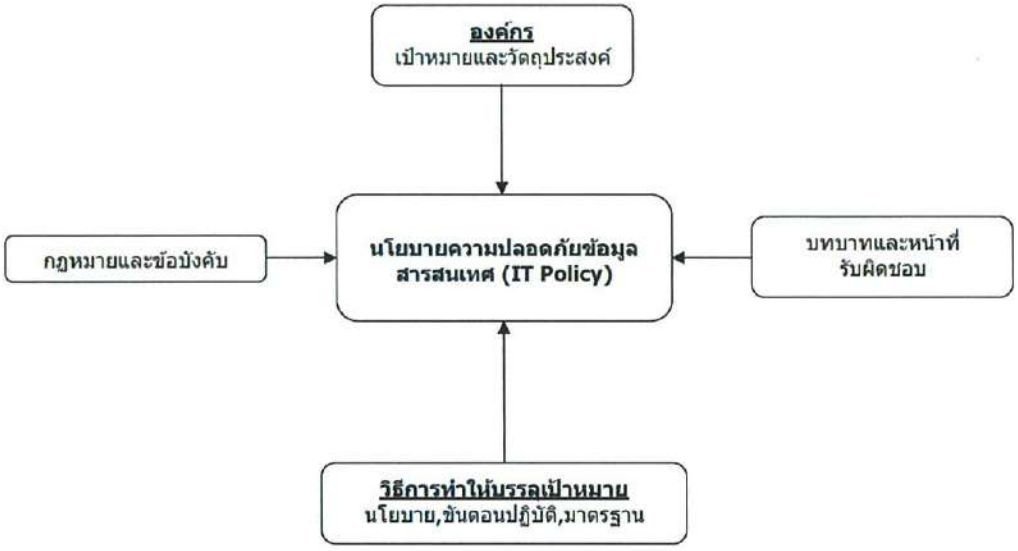
SKY ICT PUBLIC COMPANY LIMITED (Head Office)
55, A.A. Capital Ratchada Building, 5th-7th Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท สกาย ไอซีที จำกัด (มหาชน)
55 อาคาร เอ.เอ แคปปิตอล รัชดา ชั้นที่ 5-7ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400

Tel : 0-2029-7888
Fax : 0-2029-7879

3. เอกสารการปฏิบัติงานและมาตรฐานต่าง ๆ ในองค์กร ควรจะสอดคล้องกับนโยบายฉบับนี้ รวมไปถึงการตรวจจับและควบคุมไวรัสคอมพิวเตอร์ รหัสผ่าน และแผนสำรองในการดำเนินธุรกิจ
4. ข้อมูลและระบบต่าง ๆ ต้องสามารถใช้ได้และตอบสนองความต้องการทางธุรกิจได้ทุกเมื่อ
5. หน่วยงานความปลอดภัยข้อมูลมีหน้าที่รับผิดชอบในส่วนการปรับปรุงดูแลนโยบายความปลอดภัยข้อมูลฉบับนี้รวมไปถึงมาตรฐาน ขั้นตอนการปฏิบัติเพื่อให้เป็นไปตามนโยบาย และต้องสนับสนุน พร้อมให้ความช่วยเหลือกับหน่วยงานอื่นที่ทำการพัฒนางานที่เกี่ยวข้องกับความปลอดภัยของข้อมูล
6. ระดับผู้จัดการทุกคนมีหน้าที่รับผิดชอบโดยตรงในการปฏิบัติใช้นโยบายและควบคุมพนักงานที่อยู่ใต้บังคับบัญชาให้ปฏิบัติตามนโยบายอย่างถูกต้อง
7. พนักงานทุกคนจำเป็นต้องปฏิบัติตามนโยบายความปลอดภัยข้อมูลอย่างเคร่งครัด
8. บริษัทมีการควบคุมการเข้าออกภายในสำนักงานด้วยระบบตรวจสอบใบหน้า, ลายนิ้วมือหรือคีย์การ์ด โดยพนักงานจะสามารถเข้าพื้นที่ต่าง ๆ ได้ด้วยใบหน้า, ลายนิ้วมือหรือคีย์การ์ดของตนเองตามเวลาที่บริษัทกำหนดเท่านั้น
9. บริษัทมีการใช้งานระบบคอมพิวเตอร์ การเชื่อมต่ออินเทอร์เน็ต และการจัดเก็บข้อมูลการใช้งานเครือข่ายตามพรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
10. บริษัทมีบริการติดต่อสื่อสารเพื่ออำนวยความสะดวกในการทำงานของบริษัท โดยพนักงานสามารถใช้โทรศัพท์ โทรสาร อินเทอร์เน็ต ระบบเครือข่ายไร้สายและอีเมล โดยบริษัทจะสามารถจัดเก็บข้อมูลและตรวจสอบใช้งานระบบดังกล่าวได้และพนักงานจะต้องรับผิดชอบข้อมูลที่เกิดบัญชีผู้ใช้งานของตนจากการใช้งานระบบดังกล่าว
11. บริษัทจะกำหนดสิทธิ์บัญชีผู้ใช้งานของพนักงานและรหัสผ่านสำหรับการใช้งานระบบภายในสำนักงานเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบ โดยพนักงานจะต้องจัดเก็บบัญชีผู้ใช้งานของตนไว้เป็นความลับ
12. บริษัทไม่สนับสนุนการกระทำที่ผิดกฎหมายดังนั้นบริษัทจะติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องบนเครื่องคอมพิวเตอร์ของสำนักงาน และรณรงค์ให้พนักงานติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องบนเครื่องคอมพิวเตอร์พกพาของตนเองด้วย
13. เครื่องคอมพิวเตอร์ที่จะใช้งานต้องมีโปรแกรมป้องกันไวรัสที่แผนกเทคโนโลยีสารสนเทศให้การรับรอง
14. พนักงานที่ต้องการใช้งานระบบจากภายนอกสำนักงานจะต้องทำการเชื่อมต่อผ่านระบบเครือข่ายเสมือนเพื่อใช้งานระบบด้วยบัญชีผู้ใช้งานของตนเอง
15. การใช้งานเครื่องแม่ข่ายของแอพพลิเคชัน และฐานข้อมูลของระบบ ควรประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อการบรรลุวัตถุประสงค์ของการประมวลผลเท่านั้น

สารบัญ



ส่วนประกอบของความปลอดภัยข้อมูลสารสนเทศ

แผนผังด้านบนกล่าวถึงนโยบายความปลอดภัยข้อมูลสารสนเทศนั้นเป็นเอกสารที่มีเนื้อหาอ้างถึงเป้าหมาย วัตถุประสงค์ และคุณค่าขององค์กร ซึ่งมีผลต่อภาพลักษณ์ขององค์กรเป็นหลัก ดังนั้นการนำวิธีการต่าง ๆ มาประยุกต์ใช้เพื่อให้สอดคล้องกับนโยบายและทิศทางของธุรกิจจึงเป็นเรื่องที่จำเป็นต้องมีการปฏิบัติใช้จริง นอกจากนี้กฎเกณฑ์ข้อบังคับทางกฎหมายมีส่วนสำคัญในการร่างนโยบายความปลอดภัยข้อมูลฉบับนี้เช่น กฎหมายในเรื่องการป้องกันข้อมูล และเอกสารทางอิเล็กทรอนิกส์ที่มีผลบังคับใช้แล้ว เป็นต้น และสุดท้ายการกำหนดบทบาทหน้าที่ความรับผิดชอบของพนักงานในแต่ละส่วนงานที่เกี่ยวข้องก็เป็นองค์ประกอบที่สำคัญในการที่จะทำให้พนักงานสามารถทำงานได้ตรงตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

โครงสร้างการจัดการเรื่องความปลอดภัยข้อมูล

นโยบายและระเบียบขั้นตอนทั้งหมดถูกจัดเก็บในรูปแบบเอกสารที่ได้รับการอนุมัติและยอมรับจากผู้บริหาร บริษัท สกาย ไอซีที จำกัด (มหาชน) ในแง่มุมมองของนโยบายฯ นั้นมีความสำคัญกับทุกฝ่ายและทุกแผนกทั้งองค์กร ดังนั้นข้อมูลของบริษัทที่มีให้กับพนักงานและข้อมูลที่อยู่ภายใต้ความรับผิดชอบและการกระทำของพนักงานจำเป็นต้องรับการป้องกันและเก็บรักษาเป็นอย่างดี เพราะถือว่าข้อมูลเหล่านี้มีค่ายิ่งสำหรับกลุ่มองค์กรและมีความอ่อนไหวต่อความมั่นคงของกลุ่มองค์กรอีกด้วย ทั้งนี้ยังจำเป็นต้องมีการตรวจสอบความปลอดภัยของข้อมูลไม่ว่าข้อมูลนั้นจะถูกเก็บไว้ในสื่อที่ใช้เก็บรักษาข้อมูล หรือระบบที่ใช้ในการประมวลผลข้อมูล หรือแม้แต่วิธีที่ใช้โอนถ่ายข้อมูล ก็จะต้องมีการตรวจสอบ

ขอบเขต

พนักงานบริษัท

ความปลอดภัยข้อมูลเป็นเรื่องของการให้ความร่วมมือและทำงานร่วมกัน ซึ่งพนักงานในองค์กรเองต้องเห็นถึงความสำคัญ ให้ความร่วมมือและสนับสนุนในการทำงานที่เกี่ยวกับระบบข้อมูลต่าง ๆ ดังนั้นพนักงานแต่ละคนนั้นต้องยึดถึงและปฏิบัติตามนโยบายความปลอดภัยข้อมูลบริษัทและมีความเข้าใจใส่ใจกับเอกสารที่เกี่ยวข้องและได้ประกาศให้รับทราบ พนักงานบริษัทที่ไม่ใส่ใจหรือไม่ปฏิบัติตามนโยบายฉบับนี้ จะถือว่าพนักงานละเลยและจะได้รับโทษตามระเบียบของบริษัทที่ได้กำหนดไว้

ระบบ

นโยบายฯ ฉบับนี้บังคับใช้กับคอมพิวเตอร์ระบบเครือข่าย แอปพลิเคชันทุกระบบ และระบบปฏิบัติการทั้งหมดที่เป็นของบริษัท สกาย ไอซีที จำกัด (มหาชน) และดำเนินการโดยบริษัท สกาย ไอซีที จำกัด (มหาชน) และรวมไปถึงข้อมูลที่เก็บหรืออยู่ในระบบคอมพิวเตอร์และระบบเครือข่ายและทรัพยากรข้อมูลทุกชนิดที่อยู่ภายในองค์กรด้วย นโยบายฯฉบับนี้ครอบคลุมถึงข้อมูลประเภทต่าง ๆ ดังนี้

1. ข้อมูลที่ถูกเก็บไว้ในฐานข้อมูล (Database) และ เซิร์ฟเวอร์ (Servers)
2. ข้อมูลที่อยู่หรือเก็บไว้ในคอมพิวเตอร์และอุปกรณ์อื่น ๆ รวมถึงข้อมูลที่ส่งผ่านระบบเครือข่าย ไม่ว่าจะเป็นภายในองค์กรหรือภายนอกองค์กร และข้อมูลที่ส่งจากภายในองค์กรไปยังเครือข่ายสาธารณะ
3. ข้อมูลที่ถูกพิมพ์หรือเขียนด้วยลายมือ และเอกสารต่าง ๆ
4. ข้อมูลที่ส่งผ่านอีเมลหรือจดหมายอิเล็กทรอนิกส์ หรือวิธีการสื่อสารที่นอกเหนือจากนี้
5. ข้อมูลที่เก็บอยู่ในสื่อที่สามารถเคลื่อนย้ายได้ เช่น ฮาร์ดดิสก์ (Hard disk), แผ่นดิสก์เก็ต (floppy disk), แผ่นซีดีรอม (CD-ROMs), เทป และสื่อเก็บข้อมูลอื่น ๆ ที่คล้ายคลึงกัน รวมถึงสื่อที่มีการเก็บข้อมูลถาวรด้วย
6. ข้อมูลที่ถูกนำเสนอบนสไลด์ ข้อมูลฉายผ่านทางโปรเจคเตอร์ ข้อมูลที่มีการเขียนบนกระดานบอร์ด ข้อมูลที่มองเห็นได้ด้วยตาและข้อมูลได้ยินจากสื่อ
7. ข้อมูลที่ถูกเก็บในลักษณะของไฟล์ (file) ซึ่งมีนามสกุลไฟล์ต่าง ๆ กันเช่น .doc, .docx, .xls, .xlsx, .ppt, .jpg และอื่นๆ เป็นต้น
8. ข้อมูลที่ใช้พูดสื่อสารกันทางโทรศัพท์หรือในขณะมีการประชุม

บทบาทและหน้าที่รับผิดชอบ

หน้าที่ความรับผิดชอบ

หน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และ การประมวลผลข้อมูลส่วนบุคคลควรได้รับการสร้างความตระหนัก เพื่อให้ทราบถึงข้อกำหนดและภาระผูกพันในการคุ้มครองข้อมูลส่วนบุคคล

1. หน้าที่รับผิดชอบที่แยกจากกัน

   บริษัท สกาย ไอซีที จำกัด (มหาชน) นั้นต้องมีการกำหนดในเรื่องหน้าที่ความรับผิดชอบที่แตกต่างกันอย่างชัดเจน โดยเฉพาะในระบบโปรดักชัน (Production Environment) หรือระบบที่ใช้งานจริงนั้น นักพัฒนาโปรแกรม (Developer) ต้องมีหน้าที่และความรับผิดชอบที่แยกจากเจ้าหน้าที่ดูแลระบบ (System Administrator)
2. การจัดทำลักษณะงาน

   ผู้บริหารต้องจัดทำมาตรการ ขั้นตอนต่างๆ ในการทำงานทั้งแบบป้องกันและตรวจจับเกี่ยวกับการตรวจสอบความปลอดภัย และปรับปรุงปฏิบัติอย่างต่อเนื่อง เพื่อให้ข้อมูลของบริษัท สกาย ไอซีที และกลุ่มบริษัทในเครือไม่อยู่ในความเสี่ยงชั้นร้ายแรงที่เกี่ยวกับการแก้ไขข้อมูลที่ไม่ได้รับอนุญาตหรือไม่มีสิทธิ์ในการแก้ไข และทำให้ไม่สามารถตรวจจับได้ ซึ่งขั้นตอนการทำงานเหล่านี้จำเป็นต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรและจัดทำเป็นเอกสารอย่างชัดเจน
3. จัดเตรียมพนักงานสำรอง

   ในระบบการทำงานจริงจำเป็นต้องมีพนักงานที่สามารถทำงานแทนพนักงานที่ทำหน้าที่รับผิดชอบหลักได้ ในกรณีที่พนักงานมีที่รับผิดชอบหลักไม่สามารถปฏิบัติงานได้
4. กำหนดความรับผิดชอบ

   เจ้าของข้อมูลมีหน้าที่ดูแลและควบคุมข้อมูล รวมทั้งกำหนดการเข้าถึงข้อมูลที่ตนมีหน้าที่รับผิดชอบด้วยผู้บังคับบัญชาของเจ้าของข้อมูลหรือหัวหน้าแผนกของเจ้าของข้อมูล มีหน้าที่รับผิดชอบแทนเจ้าของข้อมูลในนั้นกรณีที่เจ้าของข้อมูลไม่สามารถปฏิบัติงานได้

ฝ่าย/หน่วยงานจัดการเรื่องความปลอดภัยข้อมูล

1. หน่วยงานจัดการความปลอดภัยข้อมูลมีหน้าที่ จัดทำ สนับสนุน ดำเนินการ และพัฒนาปรับปรุงนโยบายความปลอดภัยข้อมูล มาตรฐาน และให้คำแนะนำขั้นตอนการทำงานต่างๆ ที่เกี่ยวกับความปลอดภัยข้อมูลองค์กร
2. หน่วยงานนี้จะมีการปฏิบัติงานเกี่ยวกับการประเมินความเสี่ยงของระบบข้อมูลภายในองค์กรและการจัดการความเสี่ยงที่เกิดขึ้น เตรียมแผนปฏิบัติงานเกี่ยวกับระบบความปลอดภัยข้อมูล ประเมินผลิตภัณฑ์ที่ใช้ในงานความปลอดภัยข้อมูล และปฏิบัติตามแผนการที่กำหนดไว้เพื่อให้แน่ใจว่าองค์กรมีระบบความปลอดภัยข้อมูลเพียงพอ
3. ฝ่ายงานตรวจสอบภายในต้องประสานงานกับหน่วยงานจัดการเรื่องความปลอดภัยข้อมูล เพื่อให้แน่ใจว่านโยบายต่าง ๆ ที่กำหนดขึ้นนั้นสอดคล้องกับข้อบังคับและกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศ และสามารถปฏิบัติได้อย่างถูกต้อง

4. การปฏิบัติตามระเบียบข้อบังคับที่มีผลต่อข้อกฎหมายที่เกี่ยวกับความปลอดภัยข้อมูลนั้น เป็นหน้าที่ความรับผิดชอบของผู้จัดการของแต่ละหน่วยงานที่ต้องให้ความร่วมมือกับทางฝ่ายบุคคลของบริษัท สกาย ไอซีที จำกัด (มหาชน)
5. ติดตาม แก้ไข ปรับปรุงขั้นตอน วิธีการปฏิบัติในงานซึ่งเกี่ยวข้องกับความปลอดภัยข้อมูล เพื่อให้มีผลบรรลุตามวัตถุประสงค์และเป็นไปตามนโยบาย
6. รายงานความคืบหน้าของการทำงาน ช่องโหว่ที่ตรวจพบผลของนโยบายความปลอดภัยข้อมูลและข้อมูลอื่น ๆ ที่เกี่ยวข้องกับหน่วยงานตรงต่อคณะกรรมการตรวจสอบ (Audit Committee) และ/หรือประธานกรรมการบริษัท

หน้าที่รับผิดชอบของพนักงาน

พนักงานต้องคุ้นเคยและเข้าใจในนโยบายความปลอดภัยข้อมูลของบริษัท รวมถึงข้อบังคับ ระเบียบมาตรฐานต่าง ๆ ที่มีผลต่อกฎหมาย ซึ่งพนักงานต้องทำความเข้าใจเป็นอย่างดีและปฏิบัติตามให้ครบถ้วน

หน้าที่ของเจ้าของ

1. เจ้าของข้อมูลโดยทั่วไปแล้วจะอยู่ในระดับผู้บริหาร ผู้จัดการของบริษัท สกาย ไอซีที จำกัด (มหาชน) หรือสามารถมอบหมายหน้าที่นี้ให้กับผู้อื่นที่มีความรับผิดชอบโดยตรงได้ซึ่งมีหน้าที่ดูแล ครอบครอง พัฒนาแอปพลิเคชันที่ใช้งานได้จริงนั้น ๆ (ระบบที่ใช้สนับสนุนในการตัดสินใจ) เพื่อไว้ใช้ในการสนับสนุนและช่วยเหลือในการตัดสินใจต่าง ๆ และการทำงานภายในองค์กร
2. ในส่วนแอปพลิเคชันที่ใช้งานจริงนั้นจำเป็นต้องมีการแต่งตั้งผู้เป็นเจ้าของแอปพลิเคชัน
3. เจ้าของข้อมูลมีหน้าที่กำหนดประเภทของข้อมูล ซึ่งสามารถจัดประเภทตามระดับความสำคัญของข้อมูลลักษณะของข้อมูลว่ามีความเป็นความลับมากน้อยแค่ไหน และมีการกำหนดว่าข้อมูลควรถูกเก็บเพื่อใช้งานได้นานเท่าไรตามแต่ละประเภทของข้อมูล กระจัดประเภทของข้อมูลนี้รวมไปถึงการกำหนดระดับการเข้าถึงของผู้ใช้งานข้อมูลด้วย

หน้าที่ของผู้ดูแลข้อมูล

1. ผู้ดูแลข้อมูลหมายถึงพนักงานที่อยู่ในส่วนงานความปลอดภัยข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) หรือผู้ที่ถูกมอบหมายให้ทำงานในส่วนการดูแลข้อมูล
2. พนักงานในแผนกเทคโนโลยีสารสนเทศ (แผนก IT), ผู้ดูแลระบบ และพนักงานผู้ที่มีหน้าที่รับผิดชอบหรือทำงาน
3. ระบบที่มีข้อมูลที่ใช้ในการทำงานของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีผู้ดูแลอย่างเป็นทางการอย่างน้อยหนึ่งคน ผู้ดูแลมีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูล ดูแลและควบคุมในเรื่องการเข้าถึงระบบ เพื่อป้องกันผู้ที่ไม่มีสิทธิ์ในการเข้าถึง เข้าถึงข้อมูลสำคัญ และต้องมีการสำรองข้อมูลเป็นประจำ (เพื่อป้องกันปัญหาเรื่องข้อมูลหาย)

คำนิยาม

1. "**องค์กร**", "**บริษัท**" หมายถึง บริษัท สกาย ไอซีที จำกัด (มหาชน)
2. "**พนักงาน**", "**คนทำงาน**", และ "**ผู้ใช้งาน**" หมายถึง พนักงานที่ถูกว่าจ้างทุกประเภท เพื่อทำงานให้กับบริษัท สกาย ไอซีที จำกัด เช่น พนักงานประจำ, พนักงานว่าจ้างตามสัญญา, พนักงานว่าจ้างชั่วคราว, และ พนักงานว่าจ้างเป็นช่วงเวลา รวมถึงผู้บริหารในระดับต่าง ๆ ของ บริษัท สกาย ไอซีที จำกัด (มหาชน) ที่อยู่ภายใต้การว่าจ้างของบริษัท
3. "**ระบบ**" หรือ "**ระบบคอมพิวเตอร์**" หมายถึง เครื่องมือทุกชนิด, เซิร์ฟเวอร์ทุกประเภท และอุปกรณ์คอมพิวเตอร์ ทั้งในแบบมีสายและไร้สาย ทุกอย่างที่อยู่ในอุปกรณ์และสื่อบันทึกต่าง ๆ เพื่อใช้สำหรับส่งข้อมูลผ่านทางอินเทอร์เน็ต (ออกภายนอกองค์กร) เอ็กซ์ทราเน็ต (ภายในเครือข่ายที่เชื่อถือได้ที่ต่อกับองค์กร) และอินทราเน็ต (ภายในองค์กร) รวมถึงอุปกรณ์อิเล็กทรอนิกส์ทุกอย่างและอุปกรณ์โทรคมนาคมที่ใช้งานคล้ายคลึง กับคอมพิวเตอร์ ทั้งนี้ยังรวมไปถึงสิ่งของต่าง ๆ ที่เป็นทรัพย์สินของ บริษัทและกลุ่มบริษัทในเครือสกาย ไอซีที และที่เป็นของผู้ร่วมทำงานหรือหุ้นส่วน และที่เป็นของผู้ขายที่มีการซื้อ ติดตั้ง และตั้งอยู่ในพื้นที่ของ บริษัท สกาย ไอซีที จำกัด (มหาชน) ไม่ว่าสิ่งของหรืออุปกรณ์เหล่านั้นจะอยู่ในสภาวะแบบใด
4. "**ข้อมูล**" หรือ "**ข้อมูลคอมพิวเตอร์**" หมายถึง สัญญาณอิเล็กทรอนิกส์ ไฟฟ้า เสียง หรือรูปแบบอื่น ๆ ทุกชนิดที่สามารถถูกเปลี่ยนหรือแปลงให้มีความหมายเพื่อให้มนุษย์เข้าใจได้ เช่น ตัวอักษร รูปภาพนิ่งภาพเคลื่อนไหว เสียง หรือรูปแบบอื่น ๆ ที่สามารถใช้เพื่อการสื่อสารระหว่างคนด้วยกันได้โดยใช้อุปกรณ์อิเล็กทรอนิกส์ หรืออุปกรณ์คอมพิวเตอร์ในการส่งสารจากอีกที่หนึ่งไปยังอีกที่หนึ่ง หรือเก็บบันทึกไว้ในเครื่องมืออื่น ๆ และสามารถนำไปใช้ใหม่ ชั่วคราวหรือตลอดไปได้

1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY POLICY)

วัตถุประสงค์

เพื่อให้องค์กรมีการกำหนดทิศทางการบริหารจัดการและให้การสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

นโยบาย

1.1. ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

1.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) จัดทำนโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัย

ในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยนโยบายความมั่นคงปลอดภัยสารสนเทศ ดังกล่าวจะต้องได้รับการอนุมัติจากผู้บริหาร บริษัท สกาย ไอซีที จำกัด (มหาชน) และจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยสารสนเทศให้กับ พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security) นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลากำหนดไว้ (อย่างน้อย 1 ครั้งต่อปี) และกรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญให้ดำเนินการปรับปรุงนโยบายภายใน 6 เดือน

1.1.3 เพื่อให้มั่นใจว่าพนักงานในบริษัทฯ รับทราบเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำงาน

2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (ORGANIZATION OF INFORMATION SECURITY)

วัตถุประสงค์

เพื่อให้องค์กรมีการกำหนดขอบเขตการบริหารจัดการองค์กร มีการควบคุมการปฏิบัติงาน และมีการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศในองค์กร รวมทั้งการรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกล และของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

นโยบาย

2.1. โครงสร้างภายในองค์กร (Internal Organization)

2.1.1. บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ

2.1.2. การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยการทำให้มีการเปลี่ยนแปลงทรัพย์สินขององค์กร หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสเกิดขึ้นนั้น

2.1.3. การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities) การติดต่อกับหน่วยงานผู้มีอำนาจต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.4. การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน(Contact with special interest groups) การติดต่อกับกลุ่มที่มีความสนใจเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.5. ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management) การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตาม ต้องมีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

3. การควบคุม ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (HUMAN RESOURCE SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่าพนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา มีความตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง เพื่อลดความเสี่ยงจากความผิดพลาด และการนำไปใช้งานในทางที่ไม่เหมาะสมของพนักงาน และเพื่อให้มั่นใจในกระบวนการเปลี่ยนแปลงหรือสิ้นสุดการจ้างงานไม่กระทบกับความปลอดภัยสารสนเทศ

นโยบาย

3.1. ก่อนการจ้างงาน (Prior to employment)

3.1.1. การคัดเลือก (Screening) การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการ โดยมีความสอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

3.1.2. ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment) ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงาน และผู้ที่ทำสัญญาต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และขององค์กร

3.2. ระหว่างการจ้างงาน (During employment)

3.2.1. หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities) ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กรที่กำหนดไว้

3.2.2. การสร้างความตระหนัก การให้ความรู้ บุคลากรฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ(Information security awareness, education and training) พนักงานขององค์กรทั้งหมดและผู้ที่ทำสัญญาต่าง ๆ ที่เกี่ยวข้อง ต้องได้รับการสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติขององค์กรที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

3.2.3. กระบวนการทางวินัย (Disciplinary process) กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ และมีการสื่อสารให้พนักงานได้รับทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร

3.3. การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

3.3.1. การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities) หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้าง รวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

4. การควบคุม การบริหารจัดการทรัพย์สิน (ASSET MANAGEMENT)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการระบุทรัพย์สินขององค์กร และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม สารสนเทศได้รับการยกระดับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร มีการป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

นโยบาย

4.1. หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

4.1.1. บัญชีทรัพย์สิน (Inventory of assets) ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องมีการระบุ จัดทำเป็นทะเบียนทรัพย์สิน และปรับปรุงให้ทันสมัย

4.1.2. ผู้ถือครองทรัพย์สิน (Ownership of assets) ทรัพย์สินในทะเบียนทรัพย์สินต้องมีผู้ถือครองทรัพย์สิน

4.1.3. การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets) กฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร และบังคับใช้ให้เป็นไปอย่างสอดคล้อง

4.1.4. การคืนทรัพย์สิน (Return of assets) พนักงานและลูกจ้างของหน่วยงานภายนอก ทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง

4.2 การจัดชั้นความลับของสารสนเทศ (Information classification)

4.2.1. ชั้นความลับสารสนเทศ (Classification of information) สารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

4.2.2. การบ่งชี้สารสนเทศ (Labeling of information) ขั้นตอนปฏิบัติสำหรับการบ่งชี้สารสนเทศต้องมี การจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับสารสนเทศที่องค์กรกำหนดไว้

4.2.3. การจัดการทรัพย์สิน (Handling of assets) ขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

5. การควบคุม การเข้าถึง (ACCESS CONTROL)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต และมีการป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) และการป้องกันการปฏิเสธความรับผิด

นโยบาย

5.1. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

5.1.1. การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User registration and deregistration) กระบวนการลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิ์การเข้าถึง

5.1.2. การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User access provisioning) กระบวนการจัดการสิทธิ์การเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตาม ทั้งให้และถอดถอนสิทธิ์การเข้าถึงสำหรับผู้ใช้งานทุกประเภท และทุกระบบและบริการทั้งหมดขององค์กร

5.1.3. การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์ (Management of privileged access right) การให้และใช้สิทธิ์การเข้าถึงตามระดับสิทธิ์ต้องมีการจำกัดและควบคุม

5.1.4. การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ ต้องมีการควบคุมโดยผ่านกระบวนการบริหารจัดการที่เป็นทางการ

5.1.5. การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights) เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้

5.1.6. การถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึง (Removal or adjustment of access rights) สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอก ต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

5.2. **การควบคุมการเข้าถึงระบบ (System and application access control)**

5.2.1. การจัดการเข้าถึงสารสนเทศ (Information access restriction) การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

5.2.2. ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure logon procedures) กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

5.2.3. ระบบบริหารจัดการรหัสผ่าน (Password management system) การใช้งานโปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมใช้อย่างใกล้ชิด

5.2.4. การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code) การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม

6. การควบคุม การเข้ารหัสข้อมูล (CRYPTOGRAPHY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

นโยบาย

6.1. มาตรการเข้ารหัสข้อมูล (Cryptographic controls)

6.1.1. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls) นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

6.1.2. การบริหารจัดการกุญแจ (Key management) นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

7. การควบคุม ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (PHYSICAL AND ENVIRONMENTAL SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีผลต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร มีการป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

นโยบาย

7.1. พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

7.1.1. ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter) ขอบเขตหรือบริเวณโดยรอบพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่สำคัญดังกล่าว อันประกอบไปด้วยสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศที่มีความสำคัญ

7.1.2. การควบคุมการเข้าออกทางกายภาพ (Physical entry controls) พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการป้องกันโดยมีการควบคุมการเข้าออกออย่างเหมาะสม โดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถถึงพื้นที่สำคัญได้

7.1.3. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities) ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอุปกรณ์ต่าง ๆ ต้องมีการออกแบบและดำเนินการ

7.1.4. การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external and environmental threats) การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ

7.1.5. การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in secure areas) ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการจัดทำและปฏิบัติตาม

7.1.6. พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas) จุดหรือบริเวณที่สามารถเข้าถึงองค์กร เช่น พื้นที่สำหรับรับส่งสิ่งของ บริเวณอื่น ๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ขององค์กรได้ ต้องมีการควบคุม และหากเป็นไปได้ จุดหรือบริเวณดังกล่าว ควรแยกออกจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

7.2. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

7.2.1. การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection) อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัยคุมคาม และอันตรายด้านสภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.2. การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection) อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัยคุมคาม และอันตรายด้านสภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.3. ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security) การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศ ต้องมีการป้องกันจากการขัดขวางการทำงานการแทรกแซงสัญญาณ หรือการทำให้เสียหาย

7.2.4. การบำรุงรักษาอุปกรณ์ (Equipment maintenance) อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้อง เพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง

7.2.5. การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of assets) อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ต้องไม่มีการนำออกนอกสำนักงาน โดยปราศจากการขออนุญาตก่อน

7.2.6. ความมั่นคงปลอดภัยของอุปกรณ์ และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off premises) ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัย โดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน

7.2.7. ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or reuse of equipment) อุปกรณ์ที่มีสื่อบันทึกข้อมูล ต้องมีการตรวจสอบเพื่อให้มั่นใจว่า ข้อมูลสำคัญของซอฟต์แวร์ที่มีใบอนุญาต มีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

7.2.8. อุปกรณ์ของผู้ใช้งานที่ ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment) ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

7.2.9. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ เพื่อป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร

8. การควบคุม ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (OPERATION SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่าการปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย สารสนเทสและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี มีการป้องกันการสูญหายของข้อมูล มีการบันทึกเหตุการณ์และจัดทำหลักฐาน และมีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

นโยบาย

8.1. ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

8.1.1. การสำรองข้อมูล (Data backup) ข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอ ตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

8.2. การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

8.2.1. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware) มาตรการตรวจหา การป้องกัน และการกู้คืนจากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

8.2.2. ตั้งค่าให้ซอฟต์แวร์ Anti-malware อัพเดทซอฟต์แวร์ และปรับปรุงค่า Signature ทุกวัน

9. การควบคุม ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (COMMUNICATIONS SECURITY)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กร และภายนอกองค์กร

นโยบาย

9.1. การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

9.1.1. มาตรการเครือข่าย (Network controls) เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่าง ๆ

9.1.2. ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม

9.1.3. การแบ่งแยกเครือข่าย (Segregation in networks) กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

10. การควบคุม การจัดหา การพัฒนา และการบำรุงรักษาระบบ (SYSTEM ACQUISITION,DEVELOPMENT AND MAINTENANCE)

วัตถุประสงค์

เพื่อให้มั่นใจว่าความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการใช้บริการผ่านเครือข่ายสาธารณะด้วย เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

10.1. ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

10.1.1. การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification) ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว

10.1.2. ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกง การโต้เถียง และการเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

10.1.3. การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

11. การควบคุม ความสัมพันธ์กับผู้ให้บริการภายนอก (SUPPLIER RELATIONSHIPS)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงของผู้ให้บริการภายนอก

นโยบาย

11.1. ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

11.1.1. นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships) ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดตกลงกับผู้ให้บริการภายใน และจัดทำเป็นลายลักษณ์อักษร

11.1.2. การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการผู้ให้บริการภายนอก (Addressing security within supplier agreements) ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนด และตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการ โครงสร้างพื้นฐานของระบบสำหรับสารสนเทศขององค์กร โดยผู้ให้บริการภายนอก

11.1.3. ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศ และการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain) ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

12. การควบคุม การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (INFORMATION SECURITY INCIEDNT MANAGEMENT)

วัตถุประสงค์

เพื่อให้มั่นใจว่ามีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนของความมั่นคงสารสนเทศให้ได้รับทราบ

นโยบาย

12.1. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ และการปรับปรุง (Management of information security incidents and improvements)

12.1.1. หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

12.1.2. การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสม และรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

12.1.3. การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses) พนักงานและผู้ที่ทำสัญญาจ้าง ซึ่งใช้ระบบและบริการสารสนเทศขององค์กร ต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย

12.1.4. การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องมีการประเมินและต้องมีการตัดสินใจว่า สถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

12.1.5. การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

12.1.6. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents) ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

12.1.7. การเก็บรวบรวมหลักฐาน (Collection of evidence) องค์กรต้องกำหนดและประยุกต์ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหา และจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐานได้

13. การควบคุม ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการความต่อเนื่องทางธุรกิจ (INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT)

วัตถุประสงค์

เพื่อสร้างความต่อเนื่องทางธุรกิจและมีการจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

13.1. ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

13.1.1. การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity) องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ

13.1.2. การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity) องค์กรต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

13.1.3. การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity) องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

14. การควบคุม ความสอดคล้อง (COMPLIANCE)

วัตถุประสงค์

เพื่อให้มั่นใจว่าองค์กรไม่มีการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงสารสนเทศ และมีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนการปฏิบัติขององค์กร

นโยบาย

14.1. การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

14.1.1. การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security) วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และปฏิบัติขององค์กร กล่าวคือ วัตถุประสงค์มาตรการ นโยบาย กระบวนการ และขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสนเทศ ต้องมีการทบทวนอย่างอิสระ ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงองค์กรที่มาก เกิดขึ้น

14.1.2. ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards) ผู้จัดการต้องดำเนินการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

14.1.3. การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review) ระบบต้องได้รับการทบทวนอย่างสม่ำเสมอ เพื่อพิจารณาความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

15. การควบคุม การใช้อุปกรณ์ส่วนตัวในการทำงาน

วัตถุประสงค์

เพื่อให้มั่นใจว่าบริษัทมีการพิจารณาดำเนินการ การใช้อุปกรณ์ส่วนตัวในการทำงาน ให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนการปฏิบัติของบริษัท

นโยบาย

ให้มีการพิจารณาและควบคุมการนำคอมพิวเตอร์แบบพกพา สื่อบันทึกอิเล็กทรอนิกส์แบบพกพา (เช่น USB) โทรศัพท์มือถือ หรือ iPad ที่เป็นทรัพย์สินส่วนตัวมาใช้ในการทำงาน เว้นแต่ ได้ลงทะเบียนการใช้อุปกรณ์ดังกล่าวไว้กับฝ่ายเทคโนโลยีสารสนเทศแล้ว ทั้งนี้ เมื่อฝ่ายเทคโนโลยีสารสนเทศ ได้ดำเนินการตั้งค่าเครื่องอุปกรณ์ดังกล่าว เพื่อความปลอดภัยของข้อมูล และอยู่ภายใต้การควบคุม กำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศแล้ว การนำเครื่องอุปกรณ์ดังกล่าวไปใช้งาน ให้คำนึงถึงระดับความเสี่ยง และดำเนินการ ดังนี้

ระดับความเสี่ยงต่ำ	**ตัวอย่างเช่น** - **การใช้งานมีข้อมูลที่ใช้ระบุตัวบุคคลได้ เช่น อีเมล์ หรือแอพพลิเคชั่นอื่น แต่ไม่ได้อ่อนไหวมากจนจัดอยู่ในระดับที่ถ้ามีการเปิดเผย หรือนำไปใช้ในทางที่ผิดแล้ว จะส่งผลเสียต่อเจ้าของข้อมูล หรือ บริษัท** - **การใช้งานมีข้อมูลอันเป็นที่เปิดเผยแก่สาธารณะ หรือสามารถค้นหาได้จากแหล่งข้อมูลอื่นโดยง่าย**
ระดับความเสี่ยงสูง	ตัวอย่างเช่น - ข้อมูลของพนักงานตั้งแต่ 10 คนขึ้นไปที่เกี่ยวกับการประเมินผลการทำงาน การพัฒนาการศักยภาพในการทำงาน หรือข้อมูลที่เกี่ยวกับชีวิตส่วนตัว หรือครอบครัวของพนักงาน - บันทึกข้อมูลสุขภาพที่ใช้ระบุตัวบุคคลได้ - กลุ่มข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลมากกว่า 10 คนขึ้นไปที่สามารถระบุตัวได้ และสามารถนำข้อมูลกลุ่มนี้ไปปลอมแปลงหรือแอบอ้าง ตัวอย่างเช่น ข้อมูลบัญชีหรือบัตรเครดิต หมายเลขประกันสังคม ข้อมูลติดต่อ วันเกิด เงินเดือน เป็นต้น

เมื่อพนักงานที่ใช้เครื่องอุปกรณ์ส่วนตัวในการใช้งานได้ประเมินระดับความเสี่ยงตามตัวอย่างข้างต้นแล้ว ในการปฏิบัติงานด้วยอุปกรณ์ส่วนตัวดังกล่าว นอกจากจะต้องปฏิบัติตามนโยบายของบริษัทที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการใช้งานเครื่องคอมพิวเตอร์แบบพกพา หรือ สื่อบันทึกพกพา และอุปกรณ์เคลื่อนที่ประเภทต่าง ๆ แล้ว ให้ดำเนินการดังต่อไปนี้เป็นการเพิ่มเติม

การปฏิบัติงานที่มีระดับความเสี่ยงต่ำ	- ตั้งรหัสผ่าน (เช่น PIN หรือ password) เพื่อใช้อุปกรณ์ และไม่เปิดเผยรหัสดังกล่าวกับผู้อื่น - ตั้งค่าให้อุปกรณ์ล็อคอัตโนมัติเมื่อไม่มีการใช้งานเป็นเวลาหลายนาที - เฝ้าระวังอุปกรณ์อย่างเหมาะสม ไม่ทิ้งอุปกรณ์ไว้โดยไม่ดูแล - อัพเดตโปรแกรมสม่ำเสมอ - ตั้งค่าไม่ให้อุปกรณ์เชื่อมต่อโดยอัตโนมัติกับสัญญาณไร้สายที่มีความเสี่ยง และควรพิจารณาก่อนจะตัดสินใจเชื่อมต่อสัญญาณ - ให้ติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกล ในกรณีที่สูญหาย - ถ้าอุปกรณ์ของเป็นอุปกรณ์มือสอง ให้ตั้งค่าให้อุปกรณ์กลับไปที่สภาพเครื่องจากโรงงานก่อนเริ่มใช้
การปฏิบัติงานที่มีระดับความเสี่ยงสูง	- ให้ดำเนินการตามแนวทางการปฏิบัติงานที่อยู่ในระดับความเสี่ยงต่ำทุกข้อ - ในกรณีที่คนในครอบครัวใช้อุปกรณ์ที่ลงทะเบียนไว้กับบริษัทด้วย พนักงานต้องไม่ให้คนในครอบครัวเข้าถึงข้อมูลของบริษัทได้ เช่น ให้มีรหัสผ่านป้องกัน account ของตนเพิ่มขึ้นมา (ทั้งนี้ บริษัทขอความร่วมมือไม่ให้แบ่งปันอุปกรณ์ส่วนตัวที่ลงทะเบียนไว้กับบริษัทให้ผู้อื่นใช้) - จัดการและตรวจสอบข้อมูลภายในเครื่องอยู่เสมอ ทำลายข้อมูลที่ไม่จำเป็น - เมื่อพนักงานไม่ใช้อุปกรณ์นี้ต่อไปแล้ว (เช่น กรณีที่นำเครื่องอื่นมาใช้แทน) หรือเมื่อลาออกจากการเป็นพนักงาน ให้ทำการลบข้อมูลในอุปกรณ์ของผู้ใช้ออกให้หมด - เข้ารหัสอุปกรณ์ (เพื่อป้องกันการเข้าถึงข้อมูล แม้หน่วยเก็บข้อมูล (storage chips) หรือดิสก์จะถูกถอดออกไปใส่ในอุปกรณ์อื่น) - ให้ติดตั้งระบบติดตามไว้กับอุปกรณ์ในกรณีที่สูญหายหรือถูกขโมย ให้ติดตั้งระบบล้างข้อมูลที่สามารถสั่งได้จากระยะไกลให้ล้างข้อมูลภายใน 36 ชม. หรือเร็วกว่านั้น - ต้องแจ้งหากเกิดการรั่วไหลของข้อมูล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบทันที - ปรับและตั้งค่าอุปกรณ์ให้มีระบบการป้องกันที่มีประสิทธิภาพสูงสุด ใช้เวลาศึกษาและทำความเข้าใจการตั้งค่าต่าง ๆ - ถ้ามีการเข้าถึงข้อมูลของบริษัทจากสถานที่อื่น ให้ทำการออกจากระบบและหยุดการเชื่อมต่อสัญญาณทุกครั้งหลักเลิกใช้ - เปิดใช้งานโหมดสูญหาย เช่น ระบบตามหาพิกัด หรือระบบสั่งล้างข้อมูลทางไกล - ดาวน์โหลดแอพลิเคชั่นจากแหล่งที่มีความน่าเชื่อถือเท่านั้น - ในกรณีของ iPhone หรือ iPad อุปกรณ์จะถูกเข้ารหัส (encrypt) เอาไว้ โดยให้กำหนดการป้องกันโดยการตั้ง PIN - ในกรณีของแอนดรอยด์ สามารถเลือกได้ให้อุปกรณ์เข้ารหัสในลักษณะ whole-device ได้ที่ “การตั้งค่า” ของอุปกรณ์ อุปกรณ์ประเภทอื่น ๆ อาจสามารถหรือไม่สามารถตั้งค่า ให้ทำการเข้ารหัสได้

การนำคอมพิวเตอร์แบบพกพา สื่อบันทึกอิเล็กทรอนิกส์แบบพกพา โทรศัพท์มือถือ หรือ iPad ออกไปใช้นอกสถานที่ ให้ทำได้เท่าที่จำเป็น และต้องดำเนินการตามนโยบายนี้อย่างเคร่งครัด

คู่มือปฏิบัติสำหรับพนักงานและผู้ใช้งาน

นโยบายความปลอดภัยข้อมูลบริษัทได้จัดทำขึ้นในลักษณะที่ทำให้พนักงานอ่านและทำความเข้าใจได้อย่างง่ายและสะดวกมากขึ้น ดังนั้นพนักงานสามารถค้นหาในส่วนที่เกี่ยวข้องกับพนักงานเองโดยดูจากกลุ่มของพนักงาน โครงสร้างของนโยบายฉบับนี้จึงได้แบ่งออกตามกลุ่มของพนักงาน ดังต่อไปนี้

1. **กลุ่มพนักงานและผู้ใช้งานทั่วไป:** กลุ่มนี้หมายรวมคือ พนักงานทุกกลุ่มซึ่งหมายถึงพนักงานจากทุก ๆ แผนกในบริษัท สกาย ไอซีที จำกัด (มหาชน) นโยบาย หน้าที่และความรับผิดชอบที่เกี่ยวข้องกับพนักงานจะถูกจัดลำดับตามกลุ่มของพนักงานไว้พนักงานที่มีหน้าที่รับผิดชอบในแต่ละกลุ่มต้องมีความเข้าใจและปฏิบัติตามนโยบายที่กำหนดไว้อย่างเคร่งครัด
2. **กลุ่มพนักงานส่วนงานบริหารและพัฒนาทรัพยากรบุคคล (PD):** รวมถึงพนักงานที่ปฏิบัติงานในส่วนงานที่เกี่ยวข้องกับทรัพยากรบุคคล
3. **กลุ่มพนักงานว่าจ้างชั่วคราวหรือพนักงานว่าจ้างจากภายนอก:** พนักงานกลุ่มนี้รวมถึง พนักงานทุกคนที่ทำงานให้กับบริษัท สกาย ไอซีที จำกัด ทั้งในแบบระยะสั้นหรือระยะยาว แต่ไม่ใช่พนักงานประจำ ตัวอย่างของพนักงานที่อยู่ในกลุ่มนี้ เช่น ผู้ขาย (vendor) หรือ พนักงานว่าจ้างจากภายนอกมาทำงานในบริษัท
4. **กลุ่มพนักงานส่วนงานฝ่ายเทคโนโลยีสารสนเทศ (IT):** เป็นพนักงานทุกคนที่อยู่ในฝ่ายเทคโนโลยีสารสนเทศ หรือแผนกไอที

กลุ่มพนักงานและผู้ใช้ทั่วไป

การเปิดเผยข้อมูลกับบุคคลภายนอกองค์กร

1. ข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) ที่ไม่ได้กำหนดให้เป็นข้อมูลที่สามารถเปิดเผยได้ ต้องมีวิธีป้องกันไม่ให้บุคคลภายนอกเข้าถึงได้
2. การอนุญาตให้บุคคลภายนอกเข้าถึงข้อมูลขององค์กรได้นั้น ต้องมีหลักฐานยืนยันเพื่อแสดงว่า ข้อมูลเหล่านั้นได้รับการอนุญาตให้เข้าถึงได้จากบริษัท สกาย ไอซีที จำกัด (มหาชน) จริง ซึ่งบุคคลภายนอกนั้นจำเป็นต้องมีการลงนามในสัญญาเรื่องการไม่เปิดเผยข้อมูลกับบริษัทสกาย ไอซีที และ กลุ่มบริษัทในเครือและการเข้าถึงข้อมูลนั้น ๆ ต้องได้รับสิทธิ์หรือการอนุญาตจากเจ้าของข้อมูลก่อนเท่านั้น
3. ถ้ามีเหตุการณ์เกี่ยวกับการเสียหายหรือสงสัยเกี่ยวกับการละเมิดการรุกล้ำสิทธิ์ในการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผย ต้องแจ้งให้เจ้าของข้อมูลหรือผู้รับผิดชอบข้อมูลนั้น ๆ และทีมงานความปลอดภัยข้อมูลรับทราบโดยด่วน

การขอข้อมูลของบริษัทจากบุคคลภายนอก

1. การร้องขอเกี่ยวกับใบสอบถาม เอกสารทางด้านการเงิน เอกสารนโยบายภายในองค์กร ขั้นตอนปฏิบัติของการทำงานในองค์กร หรือสำหรับสำรวจตรวจสอบ และการขอสัมภาษณ์กับพนักงานภายในองค์กรถูกควบคุมโดยนโยบายฉบับนี้
2. นโยบายฉบับนี้ไม่ได้ครอบคลุมถึงข้อมูลที่เกี่ยวเนื่องกับผลิตภัณฑ์และบริการของบริษัทสกาย ไอซีทีและ กลุ่มบริษัทในเครือ ถ้าบุคคลภายนอกหรือคู่ค้าของบริษัทที่ทำการส่งข้อมูลที่เป็นความลับให้พนักงานของบริษัทเป็นการส่วนตัวนั้น ทางบริษัทจะถือว่าไม่มีส่วนรับผิดชอบใด ๆ กับข้อมูลเหล่านี้

การคัดลอกข้อมูลของบริษัท

1. ไม่อนุญาตให้พนักงานที่ไม่มีสิทธิ์ทำการคัดลอกข้อมูลหรือโปรแกรม ซอฟต์แวร์ของบริษัท โดยไม่จำเป็นหรือไม่มีเหตุผลสมควร
2. ถ้าหากผู้ที่ไม่ได้รับอนุญาตให้มีสิทธิ์ในข้อมูลนั้น ๆ กระทำการส่งต่อข้อมูลให้กับบุคคลภายนอกหรือคู่ค้าจะมีความผิดตามระเบียบของบริษัท

การป้องกันข้อมูลสำคัญจากภายนอก

ข้อมูลที่เกี่ยวข้องกับมาตรการความปลอดภัยข้อมูล ไม่ว่าจะเป็นข้อมูลที่ใช้ทำงานอยู่ในระบบต่าง ๆ และในระบบเครือข่ายของบริษัท ถือว่าเป็นข้อมูลลับ และห้ามเปิดเผยให้กับพนักงานหรือบุคคลอื่นที่ไม่มีสิทธิ์เข้าถึงข้อมูลนั้น ๆ โดยไม่ได้รับการเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลของบริษัทก่อน ตัวอย่างเช่น ห้ามเปิดเผยข้อมูลเบอร์โทรศัพท์บ้านของพนักงานแก่คู่แข่งทางการค้าโดยเด็ดขาด

การจัดประเภทของข้อมูล (สี่ประเภท)

1. การแบ่งประเภทของข้อมูลนั้นพิจารณาจากความสำคัญทางด้านความเสี่ยงของข้อมูล ซึ่งอาจจะดูได้จากความต้องการใช้งานของข้อมูลนั้น ๆ ความสำคัญหรือระดับของการป้องกันข้อมูลที่จำเป็นสำหรับข้อมูลประเภทนั้น ๆ
2. บริษัท สกาย ไอซีที จำกัด (มหาชน) ได้จัดแบ่งกลุ่มข้อมูลโดยแบ่งเป็นประเภทต่าง ๆ และทำการกำหนดระดับความเหมาะสมในการป้องกันข้อมูลแต่ละประเภท และมาตรการการป้องกันและรับผิดชอบในข้อมูลนั้น ๆ รวมถึงวิธีการเก็บรักษาข้อมูล
3. ข้อมูลต่าง ๆ ในบริษัทต้องถูกจัดให้อยู่ในประเภทดังต่อไปนี้
   - 3.1. ลับสุดยอด (ห้ามเปิดเผยโดยเด็ดขาด)
   - 3.2. เป็นความลับ
   - 3.3. ใช้ภายในเท่านั้น
   - 3.4. ทั่วไป (สามารถเปิดเผยได้)

เพื่อให้แน่ใจว่าข้อมูลได้รับการป้องกันเป็นอย่างดี พนักงานทุกคนต้องทำความคุ้นเคย และเข้าใจความหมายของประเภทของข้อมูลให้ถูกต้องและเล็งเห็นความสำคัญในการจัดประเภทของข้อมูลนี้ด้วย

การติดป้ายข้อมูล

1. บริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการติดป้ายประเภทของข้อมูลอย่างเหมาะสม ตามขั้นตอนที่ได้กำหนดไว้เบื้องต้น
2. ข้อมูลที่เป็นความลับ ไม่สามารถเปิดเผยได้ ไม่ว่าจะอยู่ในสถานะใด (ตั้งแต่ขั้นแรกเริ่มจนถึงขั้นทำลาย) ต้องระบุประเภทข้อมูลให้ชัดเจน
3. การติดป้ายต้องระบุประเภทของข้อมูล วันหมดอายุหรือระยะเวลา ของข้อมูลที่ต้องเก็บรักษาไว้ วิธีการหรือขั้นตอนในการใช้งานข้อมูลนั้น ๆ และที่ตั้งในการเก็บข้อมูล ถ้ามีแล้วแต่ความจำเป็นของ
   เอกสารส่วนใหญ่อยู่ในประเภท "ใช้ภายในเท่านั้น" ไม่จำเป็นต้องติดป้ายบอกประเภทไว้ ดังนั้นเอกสารที่ไม่ได้ติดป้ายบอกประเภทจะ ถือว่าเป็นเอกสารที่ใช้สำหรับภายในเท่านั้น

การส่งข้อมูลและการถือครองข้อมูล

1. ข้อมูลที่เป็นความลับต้องมีการควบคุมเรื่องสิทธิ์ในการเข้าถึงโดยคณะทำงานความปลอดภัยข้อมูลขององค์กร
2. ผลหรือข้อมูลที่ได้จากระบบคอมพิวเตอร์ที่เป็นความลับต้องมีการส่งถึงผู้รับไว้ด้วยเป็นการส่วนตัว ต้องได้รับการเห็นชอบและอนุญาตจากเจ้าของข้อมูลก่อนนำข้อมูลที่เป็นความลับออกนอกพื้นที่ของบริษัท ข้อมูลความลับที่อยู่ในรูปแบบเอกสารต้องเก็บไว้อย่างดีเมื่อยังไม่นำออกมาใช้งาน
3. ข้อมูลที่เป็นความลับและเปิดเผยไม่ได้ที่อาจจะอยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ที่อ่านออกได้ และรูปแบบเสียงที่สามารถได้ยินและฟังได้ เพื่อใช้ในการสื่อสารระหว่างกันต้องมีการเข้ารหัสด้วย

การยกเลิกการจัดประเภทและการลดระดับความสำคัญของข้อมูล

ข้อมูลที่ถูกยกเลิกการจัดอยู่ในประเภท "เป็นความลับ " และ "ลับสุดยอด " แล้วนั้นต้องมีการระบุและแจ้งให้บุคคลที่เกี่ยวข้องทราบ จำเป็นต้องมีการทบทวนจัดประเภทข้อมูลให้ถูกต้องอย่างน้อยปีละหนึ่งครั้ง

การทำลายข้อมูล

ข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องทำลายเมื่อไม่มีความจำเป็นต้องใช้อีกต่อไปในทางธุรกิจ หากข้อมูลที่เป็นความลับหรือไม่สามารถเปิดเผยได้นั้นไม่มีความจำเป็นในการใช้งานอีก จะต้องเก็บไว้ในที่ปลอดภัยและล็อคป้องกันการเข้าถึงได้จนกว่าจะมอบให้กับผู้ที่มีสิทธิ์ของบริษัทเป็นผู้จัดการต่อไป พนักงานต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนทำลายเอกสารหรือบันทึกต่าง ๆ ที่สำคัญของบริษัท

การยินยอมจากพนักงาน

พนักงานทุกคนทั้งพนักงานประจำและพนักงานว่าจ้างชั่วคราว ต้องยินยอมในการเซ็นยอมรับในเอกสารข้อตกลงที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูล หรือเอกสารข้อตกลงที่เกี่ยวข้องกับการไม่เปิดเผยข้อมูลของบริษัทตั้งแต่วันที่พนักงานเข้าทำงานในบริษัท สกาย ไอซีที จำกัด (มหาชน)

การควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกต่าง ๆ

1. การเข้าพื้นที่ทำงาน ห้องเก็บเครื่องมือสื่อสารโทรคมนาคม ห้องเซิร์ฟเวอร์ หรือพื้นที่ของสถานที่ทำงานที่มีการเก็บข้อมูลที่ไม่สามารถเปิดเผยได้หรือมีข้อมูลที่เป็นความลับจะต้องจำกัดสิทธิ์เฉพาะพนักงานที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้
2. ข้อมูลที่เป็นความลับต้องป้องกันจากบุคคลที่ไม่มีสิทธิ์ในการเข้าถึง
3. เอกสารที่อยู่ในรูปแบบสิ่งพิมพ์และเก็บข้อมูลที่เป็นความลับต้องถูกเก็บไว้ในตู้เอกสารที่ปิดล็อคได้
4. ข้อมูลที่เป็นความลับต้องถูกเก็บไว้ในที่ ๆ ปลอดภัยและสามารถปิดล็อคได้ระหว่างที่ไม่ได้อยู่ในช่วงเวลาทำงาน
5. แนะนำให้มีการทำนโยบายการรักษาระเบียบและความสะอาดโต๊ะทำงานเพื่อป้องกันการเข้าถึงเอกสารสำคัญ
6. หน้าจอคอมพิวเตอร์ควรจะมีการตั้งค่าของภาพที่แสดงให้เหมาะสม โดยไม่ควรแสดงหรือกำหนดภาพและเนื้อหาที่ไม่เหมาะสมบนหน้าจอคอมพิวเตอร์

การถือครองข้อมูลระหว่างการเข้ากะทำงาน

ข้อมูลที่เป็นความลับของบริษัทต้องถูกเก็บไว้ในพื้นที่ ๆ จัดไว้อย่างปลอดภัย และต้องไม่ละเลยหรือทิ้งข้อมูลเหล่านั้นไว้ในที่ ที่ไม่ปลอดภัยในช่วงของกะทำงานเวลาถัดไป

การตรวจสอบทรัพย์สินก่อนนำออก

ต้องมีการตรวจสอบหรือได้รับอนุญาตให้นำอุปกรณ์คอมพิวเตอร์หรือชิ้นส่วนคอมพิวเตอร์ก่อนจะนำออกจากพื้นที่ของบริษัทได้

สิทธิ์ในการตรวจสอบและระวังภัย

1. ผู้จัดการหรือหัวหน้างานมีสิทธิ์ในการตรวจสอบหรือตรวจตราการใช้งานระบบที่เกี่ยวข้องกับข้อมูลของบริษัททุกเวลา
2. การตรวจสอบในลักษณะนี้อาจจะได้รับการยินยอมหรือไม่ยินยอมจากพนักงานคนนั้น ๆ ก็ตาม
3. ระบบข้อมูลต่าง ๆ ของบริษัทสามารถตรวจสอบโดยดูจาก การใช้งานการทำงานของพนักงานที่บันทึกไว้ จากข้อมูลไฟล์ที่อยู่ในฮาร์ดดิสก์ และข้อมูลจากอีเมลหรือจดหมายอิเล็กทรอนิกส์ทั้งนี้เอกสารต่าง ๆ ที่ถูกพิมพ์ หรือข้อมูลที่อยู่ในลิ้นชักโต๊ะและพื้นที่ที่ใช้เก็บข้อมูลก็สามารถถูกตรวจสอบได้เช่นกัน
4. การตรวจสอบในลักษณะนี้ต้องได้รับการอนุญาตจากหน่วยงานกฎหมายและความปลอดภัยข้อมูลก่อน
5. ผู้จัดการหรือหัวหน้างานมีสิทธิ์ที่จะริบหรือยึดสิ่งของที่ผิดต่อระเบียบนโยบายบริษัทหรือผิดต่อกฎหมาย เพื่อทำการตรวจสอบและส่งคืนเมื่อทำการตรวจสอบเรียบร้อยแล้ว

ความเป็นเจ้าของในทรัพย์สิน

1. บริษัท สกาย ไอซีที จำกัด (มหาชน) ถือเป็นเจ้าของกรรมสิทธิ์ในเรื่องสิทธิบัตร ลิขสิทธิ์ สิ่งประดิษฐ์คิดค้นหรือทรัพย์สินทางปัญญาที่สร้างหรือทำขึ้นโดยพนักงานของบริษัท
2. โปรแกรมและเอกสารทุกอย่างที่จัดทำหรือสร้างขึ้นเพื่อใช้ประโยชน์ในบริษัทโดยพนักงานของบริษัท ถือว่าเป็นกรรมสิทธิ์และทรัพย์สินของบริษัททั้งหมด และบริษัทสามารถกำหนดสิทธิ์ในการเข้าถึงหรือใช้งานข้อมูลเหล่านั้นได้ตามเห็นสมควร

การเข้าถึงอินเทอร์เน็ต

1. บริษัท สกาย ไอซีที จำกัด (มหาชน) ทุกคนสามารถเข้าอินเทอร์เน็ตได้จากเครื่องคอมพิวเตอร์ตั้งโต๊ะที่จัดไว้ให้ซึ่งการเข้าถึงนี้สามารถยกเลิกได้ทุกเมื่อตามแต่ความเห็นชอบของผู้บริหาร
2. การเข้าถึงอินเทอร์เน็ตจะถูกตรวจสอบการใช้งานให้เป็นไปอย่างเหมาะสมตามสมควร และปฏิบัติตามนโยบายความปลอดภัยข้อมูลของบริษัท
3. ห้ามมีการแสดงถึงความเป็นบริษัทหรือกลุ่มในบริษัทในที่สาธารณะโดยไม่ได้รับการอนุมัติหรือเห็นชอบจากผู้บริหารที่รับผิดชอบก่อน
4. ข้อมูลต่าง ๆ ที่ได้รับผ่านทางอินเทอร์เน็ตควรจะมีการตรวจสอบก่อนว่าได้รับมาจากแหล่งที่เชื่อถือได้จริง
5. ห้ามมีการนำสิ่งของหรือสัญลักษณ์ที่แสดงถึงตัวบริษัทหรือข้อมูลของบริษัทไปแสดงในระบบประมวลผลข้อมูลสาธารณะโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลและฝ่ายความปลอดภัยข้อมูลก่อน
6. ข้อมูลที่เป็นความลับ ไม่สามารถเปิดเผยได้ เช่น รหัสผ่านและเลขบัตรเครดิต ไม่ควรส่งผ่านทางอินเทอร์เน็ตโดยวิธีใด ๆ โดยไม่ได้ทำการเข้ารหัสก่อน

จดหมายอิเล็กทรอนิกส์หรืออีเมล

1. บริษัท สกาย ไอซีที จำกัด (มหาชน) ให้พนักงานในบริษัททุกคนมีการใช้จดหมายอิเล็กทรอนิกส์โดยมีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์และให้บริการในการรับส่งอีเมล เพื่อประโยชน์และเพิ่มความสะดวกในการการทำงานของพนักงานเอง
2. การสื่อสารที่เกี่ยวข้องกับธุรกิจของบริษัทต้องรับส่งกันโดยใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของ บริษัท
3. การใช้งานบัญชีผู้ใช้ส่วนตัว เช่น Yahoo, Hotmail ไม่อนุญาตให้นำมาใช้กับธุรกิจของบริษัท
4. ไม่อนุญาตให้มีการส่งจดหมายอิเล็กทรอนิกส์ที่เข้าข่ายล่อลวง หรือไม่มีสาระสำคัญทางธุรกิจให้กับลูกค้า
5. ทุกคนในองค์กรต้องใช้ลายเซ็นกำกับด้านล่างของจดหมายอิเล็กทรอนิกส์ให้เป็นมาตรฐาน ซึ่งประกอบไปด้วย ชื่อแรก นามสกุล ตำแหน่งการทำงาน ที่อยู่บริษัทและเบอร์โทรศัพท์ให้ชัดเจน

การเจาะข้อมูลในระบบ

พนักงานต้องไม่กระทำการเจาะข้อมูลในระบบของบริษัท สกาย ไอซีที จำกัด หรือกระทำพฤติกรรมที่คล้ายคลึงกับการตั้งใจเจาะข้อมูลในระบบ ซึ่งรวมถึงการพยายามเข้าถึงข้อมูลทั้ง ๆ ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลนั้น ๆ แม้กระทั่งพยายามสร้างความเสียหาย พยายามเปลี่ยนแปลงให้กับข้อมูล หรือสร้างความยุ่งยากให้เกิดขึ้นภายในระบบที่ใช้งานจริง และการพยายามสืบหาใช้รหัสผ่านของบุคคลอื่นหรือพยายามถอดรหัสกุญแจของระบบ และไม่ว่าการจะใช้วิธีการเข้าถึงหรือควบคุมระบบโดยไม่ได้รับอนุญาตและไม่ได้รับสิทธิ์ ทั้งหมดถือว่าเป็นการพยายามเจาะข้อมูลในระบบทั้งสิ้น

จัดระเบียบการใช้ซอฟต์แวร์

ทุกซอฟต์แวร์ที่ทำการติดตั้งในระบบของบริษัท สกาย ไอซีที จำกัด (มหาชน) และมีจัดให้พนักงานใช้หลายคนในเวลาเดียวกันต้องมีการจัดระเบียบการใช้งานและกำหนดสิทธิ์ในการเข้าถึงของพนักงานก่อนที่จะมีการเข้าถึง
ซอฟต์แวร์นั้น ๆ ได้จริง

สิทธิ์เริ่มต้นในการเข้าถึงไฟล์และระบบงานต่างๆ

เพื่อเป็นการควบคุมสิทธิ์ในการเข้าถึงข้อมูล จากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงระบบเครือข่ายของ บริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการกำหนดค่าเริ่มต้นเป็นผู้ที่ไม่มีสิทธิ์เข้าถึงเสมอ

การควบคุมการเข้าถึงผิดพลาด

ถ้าคอมพิวเตอร์หรือระบบการควบคุมการเข้าถึงข้อมูลทำงานผิดพลาดหรือไม่สามารถทำงานได้ตามปกติ ระบบต้องมีการตั้งค่าเริ่มต้นเป็นปฏิเสธการเข้าถึงจากผู้ใช้งานทั้งหมดทันที

การกำหนดและรับรองการเป็นตัวตนของผู้ใช้งาน (User ID and password [ID Management Security Policy])

1. บริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องกำหนดให้พนักงานทุกคนเข้าถึงระบบที่เกี่ยวข้องกับข้อมูลบริษัทด้วยการใช้บัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของพนักงานเองเท่านั้น
2. บัญชีผู้ใช้งาน (User ID) ถูกใช้เพื่อกำหนดเรื่องของสิทธิ์ในการเข้าถึงระบบต่าง ๆ ขึ้นอยู่กับหน้าที่รับผิดชอบลักษณะการทำงานของพนักงานแต่ละคน
3. พนักงานทุกคนในองค์กรต้องรับผิดชอบที่จะปกป้องบัญชีผู้ใช้งาน (User ID) และรหัสผ่าน (Password) ของตัวเอง
4. การจัดเก็บรหัสผ่านของผู้ใช้งานในระบบ บริษัทฯใช้วิธีการแฮช (Hash) โดยใช้ Algorithm ที่ปลอดภัย

วิธีการตั้งรหัสผ่าน

ผู้ใช้งานระบบทุกคนต้องตั้งรหัสผ่านของตัวเอง โดยรหัสผ่านนั้นควรจะยากต่อการคาดเดา และไม่ควรมีข้อมูลส่วนตัวประกอบในรหัสผ่านนั้น ตัวอย่างเช่น เลขรหัสพนักงาน เลขบัตรประชาชน เลขบัตรสุขภาพ PIN code เบอร์โทรศัพท์ ชื่อคู่ครอง ชื่อแฟน รหัสไปรษณีย์ ชื่อสถานที่ต่าง ๆ หรือศัพท์เทคนิค ศัพท์ในพจนานุกรม ไม่ควรนำมาใช้เป็นรหัสผ่านการตั้งรหัสผ่านที่ดี มีเทคนิคดังนี้:

1. ใช้คำบางคำเป็นส่วนประกอบ
2. ใช้ตัวหนังสือภาษาอังกฤษตัวเล็กหรือตัวใหญ่ หรือใช้ตัวเลขคั่นสลับกัน
3. เปลี่ยนคำธรรมดาให้เป็นคำที่มีตัวอักษรอื่นแอบแฝง
4. สามารถสร้างเป็นตัวย่อจากคำเต็มได้เอง เช่น CEGEP โดยไม่มีใครรู้ความหมาย
5. ใช้คำที่สะกดผิดเป็นส่วนประกอบ
6. ใช้เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

การใช้รหัสผ่านที่คล้ายคลึงรหัสเดิม

ผู้ใช้งานไม่ควรจะตั้งรหัสผ่านที่เหมือนกับรหัสผ่านเดิม หรือตั้งรหัสซ้ำสำหรับการเข้าถึงระบบใด ๆ ก็ตาม และไม่ควรคล้ายคลึงกับรหัสผ่านเดิมที่เคยใช้งานมาก่อนแล้ว

ข้อบังคับในการตั้งรหัสผ่าน

1. รหัสผ่านต้องมีอย่างน้อย 8 ตัวและต้องมีการเปลี่ยนรหัสผ่านทุก ๆ 180 วันหรืออาจจะน้อยกว่านี้
2. ระบบการจัดการเรื่องรหัสผ่านต้องมีการกำหนดให้ผู้ใช้งานตั้งรหัสผ่านโดยใช้ตัวอักษร ตัวเลขและอักขระพิเศษเป็นอย่างน้อยและต้องไม่อนุญาตให้มีการใช้รหัสผ่านซ้ำจากเดิมที่เคยตั้งมาแล้วหรืออย่างน้อยต้องเว้นไประยะหนึ่งถึงจะอนุญาตให้ใช้ซ้ำได้

การเก็บรักษารหัสผ่าน

1. รหัสผ่านไม่ควรเก็บไว้ในเอกสารหรือที่ ๆ เก็บแล้วสามารถนำออกมาอ่านได้ ไม่ว่าจะเป็นการเก็บเข้าแฟ้ม มาโครในซอฟต์แวร์ต่าง ๆ ในคอมพิวเตอร์ของผู้ใช้งานเอง โดยไม่มีการควบคุมการเข้าถึงเป็นอย่างดี หรือทำให้มีบุคคลที่ไม่มีสิทธิ์สามารถเข้าถึงสถานที่เก็บรหัสผ่านได้
2. รหัสผ่านควรจะไม่จดออกมาใส่กระดาษและไม่ทิ้งไว้ในที่โล่งแจ้งหรือในที่ ๆ สามารถมองเห็นได้โดยทั่วไป เช่น แปะไว้ที่หน้าจอคอมพิวเตอร์ หรือที่โต๊ะทำงาน เป็นต้น

การร่วมใช้รหัสผ่าน

1. ถ้าข้อมูลที่มีความจำเป็นต้องมีการใช้งานร่วมกัน พนักงานสามารถทำได้โดยใช้อีเมลของบริษัทหรือจดหมายอิเล็กทรอนิกส์ ฐานข้อมูล ไดเร็กทรอรีสาธารณะ ที่เก็บอยู่ในเซิร์ฟเวอร์ของบริษัท หรืออยู่ในอุปกรณ์บันทึกข้อมูลหรืออุปกรณ์ที่ใช้ในการส่งต่อหรือแลกเปลี่ยนข้อมูลกัน
2. รหัสผ่านต้องไม่มีบอกผู้อื่นที่ไม่ใช่เจ้าของ ห้ามเปิดเผยให้ผู้อื่นทราบ
3. เจ้าหน้าที่ดูแลระบบหรือเจ้าหน้าที่ ทางเทคนิค ไม่ควรสอบถามรหัสผ่านหรือเปิดเผยรหัสผ่านของพนักงานคนอื่น ๆ ยกเว้นแต่จะมีการใช้รหัสผ่านนั้นชั่วคราวเพื่อจุดประสงค์ในการทำงาน และต้องมีการเปลี่ยนรหัสผ่านนั้นทันทีหลังจากที่มีการเข้าใหม่อีกครั้งของพนักงานคนนั้น
4. ถ้าผู้ใช้งานสงสัยว่ามีบุคคลอื่นกำลังใช้บัญชีผู้ใช้ (User ID) และรหัสผ่าน (Password) ของตัวเองอยู่ จะต้องแจ้งให้เจ้าหน้าที่ที่รับผิดชอบทราบโดยด่วน

การกำจัดไวรัสคอมพิวเตอร์

1. เมื่อพนักงานได้พบเจอไวรัสที่เครื่องคอมพิวเตอร์ของตัวเอง ต้องทำการหยุดไวรัสตัวนั้นทันทีเพื่อไม่ให้ระบบหรือเครื่องคอมพิวเตอร์อื่นได้รับไวรัสด้วย และทำการแจ้งหน่วยงาน IT ทันที
2. ถ้าหากแผ่นบันทึกข้อมูล หรืออุปกรณ์เครื่องบันทึกข้อมูลที่มีการใช้งานกับเครื่องคอมพิวเตอร์ที่ติดไวรัสแล้ว ไม่ควรนำมาใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นโดยเด็ดขาด จนกว่าจะมีการลบไวรัสออกเรียบร้อยแล้ว
3. เครื่องคอมพิวเตอร์ที่ติดไวรัสต้องถูกกักกัน หรือแยกออกจากระบบเครือข่ายของบริษัท โดยทำการดึงสาย LAN ออกจากเครื่อง หรือปิด Wi-Fi
4. ผู้ใช้งานต้องไม่พยายามลบไวรัสด้วยตัวท่านเอง
5. พนักงาน IT หรือเจ้าหน้าที่รับผิดชอบมีหน้าที่ในการนำไวรัสออกจากเครื่อง อย่างเป็นขั้นตอนเพื่อให้เครื่องคอมพิวเตอร์เกิดความเสียหายน้อยที่สุด

การป้องกันไวรัส

ปัจจุบันได้มีการติดตั้งโปรแกรมตรวจจับไวรัสไว้ที่เครื่องเซิร์ฟเวอร์ทุกเครื่องและมีการทำงานตลอดเวลา เครื่องคอมพิวเตอร์ที่ไม่ได้ทำการอัพเดตเวอร์ชันในการให้รู้จักไวรัสในปัจจุบัน ไม่อนุญาตให้เชื่อมต่อกับระบบของบริษัท สกาย ไอซีที จำกัด (มหาชน) โดยเด็ดขาด ผู้ใช้งานต้องไม่ทำการดาวน์โหลดโปรแกรมหรือซอฟต์แวร์จากเว็บไซต์หรือที่อื่น ๆ ในอินเทอร์เน็ต ยกเว้นแต่เว็บไซต์นั้นจะเป็นเว็บไซต์ที่เชื่อถือได้และได้รับการอนุญาตจากหน่วยงานความปลอดภัยข้อมูลของบริษัทก่อน

การให้ความรู้แก่พนักงานในองค์กร

1. พนักงานในองค์กรทุกคนต้องได้รับการให้ความรู้และความเข้าใจพื้นฐานในนโยบายต่าง ๆ มาตรฐาน และขั้นตอนการดำเนินงานของบริษัท ทั้งนี้พนักงานทุกคนต้องได้รับความรู้เกี่ยวกับข้อมูลความปลอดภัยในปัจจุบันผ่านจากสื่อต่าง ๆ เช่น จากการทำอบรมภายในบริษัท จากทางอีเมลหรือจดหมายอิเล็กทรอนิกส์หรือจากการประกาศบนหน้าเว็บภายในของบริษัท หรือตามป้ายติดภายในบริษัทเอง
2. เนื่องจากพนักงานควรจะได้รับความรู้ในรูปแบบที่แตกต่างกัน โดยแยกตามระดับการทำงานได้ 3 ระดับดังนี้
   2.1. ระดับผู้บริหาร
   2.2. ระดับพนักงานเทคนิค
   2.3. ระดับพนักงานทั่วไป

กลุ่มพนักงานส่วนงานบริหารและพัฒนาทรัพยากรบุคคล (PD)

ความปลอดภัยที่เกี่ยวเนื่องกับขอบเขตการทำงานและพัฒนาทรัพยากรบุคคล

1. กำหนดขอบเขตและลักษณะงานของแต่ละตำแหน่งต่าง ซึ่งหมายถึงงานที่รับผิดชอบหลักงานที่เกี่ยวข้องกับส่วนงานหรือหน่วยงานอื่น และทักษะความสามารถ ประสบการณ์ที่จำเป็นสำหรับความรับผิดชอบต่อตำแหน่งงานนั้นขอบเขตและลักษณะงานนี้ต้องมีการทบทวนและแก้ไขหน้าที่ความรับผิดชอบให้ถูกต้องตามตำแหน่งงานที่เปลี่ยนแปลงไป
2. ขั้นตอนการว่าจ้างพนักงานใหม่ในตำแหน่งใด ๆ ต้องมีหลักฐานเอกสารให้ตรวจสอบได้ชัดเจน ขั้นตอนการตรวจสอบเรื่องของคุณสมบัติ แหล่งอ้างอิง การศึกษา ประวัติทางคดีการเงินและอาชญากรจำเป็นต้องมีการทบทวนและตรวจสอบเป็นอย่างดี
3. จัดให้มี Code of conduct สำหรับกำหนดพนักงานผู้มีสิทธิ์เข้าถึงข้อมูลและวิธีการเข้าถึงข้อมูล
4. จัดให้มีขั้นตอนการตรวจสอบและจัดทำ ความยินยอม (Consent Form) ให้กับพนักงาน
   1. PD Employee Consent Form 1
   2. PD Employee Consent Form 2
   3. PD Employee Consent Form 3
   4. PD Applicant Consent Form

กลุ่มพนักงานว่าจ้างชั่วคราว หรือพนักงานว่าจากภายนอก

การใช้บัญชีเข้าระบบของพนักงานชั่วคราวหรือจ้างจากภายนอก

บุคคลใดๆ ที่ไม่ใช่พนักงานประจำหรือพนักงานว่าจ้างตามสัญญา หรือที่ปรึกษาของบริษัท ไม่มีสิทธิ์ในการใช้บัญชีใช้งานเข้าระบบ (User ID) หรือไม่มีสิทธิ์ในการใช้ระบบคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ของบริษัท สกาย ไอซีที จำกัด (มหาชน) จนกว่าจะได้รับการอนุญาตจากหน่วยงานที่เกี่ยวข้องเป็นลายลักษณ์อักษรก่อน

การควบคุมการเข้าถึงระบบ

การเข้าถึงระบบภายในหรือข้อมูลของบริษัทโดยบุคคลภายนอกในแบบที่ไม่เป็นทางการต้องได้รับอนุญาตจากผู้ประสานงานหรือผู้รับผิดชอบของหน่วยงานความปลอดภัยข้อมูลก่อนล่วงหน้า ก่อนที่บุคคลภายนอกจะทำการติดต่อหรือเชื่อมต่อกับระบบของบริษัทผ่านทางเครือข่ายคอมพิวเตอร์แบบ Real-time ต้องได้รับอนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

ข้อเสนอและเงื่อนไขสำหรับการทำสัญญากับบริษัทคู่ค้า

การทำสัญญากับบริษัทคู่ค้าหรือบุคคลภายนอกต้องระบุในเรื่องของข้อเสนอและเงื่อนไขต่าง ๆ เกี่ยวกับการเข้าถึงระบบของบริษัท และมีการเซ็นรับรองจากระดับผู้จัดการของบริษัทคู่ค้าบริษัทนั้นด้วย และมีการเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลและแผนกกฎหมายของบริษัท สกาย ไอซีที จำกัด (มหาชน)

การปฏิบัติตามนโยบายความปลอดภัยข้อมูล

ที่ปรึกษา คู่สัญญา และพนักงานว่าจ้างชั่วคราวต้องปฏิบัติตามข้อกำหนดและนโยบายความปลอดภัยข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) และมีหน้าที่ความรับผิดชอบเสมือนเป็นพนักงานของบริษัท สกาย ไอซีที จำกัด (มหาชน)

ข้อตกลงในการไม่เปิดเผยข้อมูลของ บริษัท สกาย ไอซีที จำกัด (มหาชน)

การสื่อสารที่ต้องเปิดเผยข้อมูลภายในของบริษัทกับบุคคลภายนอกหรือคู่ค้าบริษัทอื่น ต้องมีการเซ็นข้อตกลงในการไม่เปิดเผยข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) จากบริษัทหรือบุคคลภายนอกก่อน ข้อมูลที่ให้กับบุคคลภายนอกหรือบริษัทคู่ค้าอื่น ต้องมีการจำกัดเรื่องของขอบเขตให้อยู่ในส่วนงานหรือเกี่ยวข้องกับส่วนงานที่ทำเท่านั้น และการเปิดเผยข้อมูลหรือให้ข้อมูลนี้ต้องได้รับการอนุญาตจากเจ้าข้อมูลก่อนเสมอ

ข้อตกลงในการไม่เปิดเผยข้อมูลของบริษัทคู่ค้า

ในกรณีที่ทางบริษัทคู่ค้ามีนโยบายให้พนักงานของบริษัท สกาย ไอซีที จำกัด (มหาชน) เซ็นลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูลของบริษัทคู่ค้านั้น ผู้ที่ได้รับเอกสารฉบับนั้นต้องส่งต่อให้ทางแผนกกฎหมายตรวจสอบซึ่งทางพนักงานของฝ่ายกฎหมายจะเป็นผู้ลงนามในเอกสารนั้นเอง

รายการการควบคุมการใช้งานระบบจัดจ้างภายนอก

ข้อตกลงที่ระบุในสัญญาทุกฉบับกับทางบริษัทจัดทำระบบจัดจ้างภายนอก ต้องมีการกำหนดเงื่อนไขให้ บริษัท สกาย ไอซีที จำกัด (มหาชน) ได้รับรายการความคิดเห็นเกี่ยวกับผลจากการควบคุมการทำงานของบริษัทที่จัดทำระบบจัดจ้างภายนอกนั้นเป็นประจำทุกปี

ผู้ให้บริการใช้ซอฟต์แวร์แอปพลิเคชัน

ทุกแอปพลิเคชันใช้ในงานจริงและมีข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) อยู่ต้องมีใบอนุญาตในการใช้งานซอฟต์แวร์นั้นอย่างถูกต้องจากผู้ให้บริการหรือเจ้าของซอฟต์แวร์นั้น และต้องมีการให้ซอร์สโค้ดเวอร์ชันล่าสุดกับบริษัทรวมถึงเอกสารรายละเอียดขั้นตอนต่าง ๆ เกี่ยวกับแอปพลิเคชันนั้น ๆ ด้วย

ผู้ให้บริการสำรอง

ถ้าเกิดกรณีฉุกเฉินเกี่ยวกับระบบการทำงานข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) ผู้ให้บริการสำรองต้องพร้อมในการรับมือกับเหตุการณ์ลักษณะนี้เสมอ โดยเฉพาะในกรณีบริษัทจัดจ้างภายนอกที่ใช้บริการอยู่ไม่สามารถทำงานหรือส่งงานตามกำหนดได้

แผนสำรองในการให้บริการของผู้ให้บริการ

สัญญาทุกฉบับที่ทำกับบริษัทให้เช่าเว็บไซต์ ผู้ให้บริการการจัดการระบบต่าง ๆ และบริษัทจัดจ้างภายนอกเกี่ยวกับระบบข้อมูลต่าง ๆ ของบริษัท ต้องมีการจัดทำแผนสำรองเป็นเอกสารอย่างชัดเจนและมีการทดสอบใช้ระบบสำรองนั้นจริงเป็นประจำตามแผนที่กำหนด

กลุ่มพนักงานส่วนงานฝ่ายเทคโนโลยีสารสนเทศ (IT)

การกำหนดสิทธิ์การใช้งานแอปพลิเคชันและการเข้าถึงข้อมูล

1. การเข้าถึงในพื้นที่สงวนหรือเขตรักษาความปลอดภัยไม่ว่าเป็นทางกายภาพ (physical access) หรือไม่ใช่ทางกายภาพ (logical access) และการเข้าถึงจากทางไกล (remote access) ต้องมีวิธีการควบคุมโดยใช้วิธีการให้แสดงตัวตนของผู้เข้าถึงอย่างเข้มงวด (identification method) และวิธีการตรวจสอบความเป็นตัวตนจริง (authentication method) ของการเข้าถึงนั้น วิธีการตรวจสอบความเป็นตัวตนต้องถูกกำหนดโดยวิธีการเข้าถึงที่เป็นมาตรฐาน ซึ่งอาจจะต้องใช้วิธีการเข้ารหัสลับในการป้องกันผู้อื่นล่วงรู้
2. พนักงานทุกคนต้องได้รับระดับและสิทธิ์ในการใช้งาน (authorization) เพื่อเข้าถึงแอปพลิเคชันและระบบต่าง ๆ ในบริษัทอย่างเหมาะสม ทุกระดับและสิทธิ์ในการใช้งานต้องได้รับการอนุมัติจากเจ้าของข้อมูลหรือผู้มีอำนาจในการให้เข้าถึง หรือผู้จัดการโปรเจคนั้น ๆ ก่อนเสมอ
3. วิธีการตรวจสอบความเป็นตัวตน (Authentication method) และวิธีการกำหนดสิทธิ์ (authorization method)ในทุก ๆ แอปพลิเคชันและระบบต่าง ๆ ในบริษัทเหล่านี้ ต้องมีการทบทวนการใช้งานสิทธิ์อย่างเป็นประจำ
4. ต้องมีการบันทึกล็อก (log) การตรวจสอบความเป็นตัวตนของผู้ใช้งานระบบและเก็บไว้ในที่ ๆ ปลอดภัย

วิธีการป้องกันการขโมย

1. อุปกรณ์เกี่ยวกับระบบการใช้งานและเครือข่าย ที่ติดตั้งอยู่ในที่โล่งแจ้ง ต้องมีการป้องกันการขโมยทางด้านกายภาพเป็นอย่างดี
2. เซิร์ฟเวอร์ในระบบเครือข่าย (LAN) และระบบสำหรับใช้งานได้หลายคนต้องถูกติดตั้งและเก็บไว้ในห้องที่สามารถปิดล็อคได้

อุปกรณ์คอมพิวเตอร์และการควบคุมคอมพิวเตอร์

1. อุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์ที่ใช้งานกับระบบจริงต้องถูกเก็บและติดตั้งในพื้นที่สงวนหรือพื้นที่ ๆ มีความปลอดภัย ที่มีทั้งความปลอดภัยในแง่เครือข่าย ความปลอดภัยในระบบและความปลอดภัยในการพิมพ์งาน

การสร้างศูนย์คอมพิวเตอร์

การสร้างศูนย์คอมพิวเตอร์ใหม่หรือการปรับปรุงนั้น ต้องคำนึงถึงการป้องกันความเสียหายที่เกิดขึ้นจากไฟไหม้จากน้ำ จากการบุกรุกหรือทำลายทรัพย์สินจากบุคคลภายนอก และจากภัยต่าง ๆ ที่คาดว่าจะเกิดขึ้น หรืออาจจะเกิดขึ้นกับสถานที่ใกล้เคียงหรือที่เกี่ยวข้องได้

การจ่ายไฟฟ้า

คอมพิวเตอร์ทุกเครื่องที่ใช้ในการบริการลูกค้าโดยตรงต้องมีการใช้ไฟสำรองจากระบบจ่ายไฟฟ้าที่ดี ฟิลเตอร์ หรือตัวระงับการกระชากไฟ ที่ได้รับการเห็นชอบจากหน่วยงานเทคโนโลยีสารสนเทศ

ความชื้นและการควบคุมอุณหภูมิ

เครื่องปรับอากาศทุกเครื่องในศูนย์คอมพิวเตอร์ต้องมีตัวอุปกรณ์ปรับอุณหภูมิให้คงที่และควบคุมความชื้นตลอด 24 ชั่วโมงต่อวัน

การป้องกันความเสียหายที่เกิดจากน้ำ

ศูนย์คอมพิวเตอร์ต้องสร้างมาเพื่อป้องกันความเสียหายที่เกิดจากน้ำ ซึ่งจะต้องมีสัญญาณเตือนภัยเป็นขั้นต่ำและกำหนดโดยหน่วยงานความปลอดภัยข้อมูล ศูนย์คอมพิวเตอร์ต้องยกพื้นให้สูงกว่าพื้นราบปกติและสูงกว่าระดับน้ำที่จะสามารถท่วมถึง (กรณีที่มีวิธีการระบายน้ำ) และต้องตั้งให้อยู่สูงกว่าท่อน้ำ หรือไม่ตั้งอยู่ใกล้กับถังเก็บกักน้ำโดดเด็ดขาด

การใช้สอยอย่างปลอดภัยหรือการนำมาใช้ใหม่ของอุปกรณ์

หน่วยงานความปลอดภัยข้อมูลต้องทำการแยกข้อมูลสำคัญหรือข้อมูลลับของบริษัทออกจากส่วนงานของระบบที่ใช้กับทางธุรกิจก่อนที่จะนำออกสู่ภายนอกหรือ ติดต่อกับทางบริษัทคู่ค้า ผู้จัดการแผนกมีหน้าที่จัดการทรัพยากรที่ไม่เป็นประโยชน์ต่อกิจกรรมทางธุรกิจโดยเป็นไปตามขั้นตอนที่ทางหน่วยงานความปลอดภัยข้อมูลจัดทำไว้ รวมถึงการย้ายข้อมูลหรือซอฟต์แวร์ที่ไม่สามารถนำมาใช้งานได้อีกด้วย

ความปลอดภัยในการสื่อสารผ่านระบบเครือข่าย

1. การเชื่อมต่อระบบเครือข่ายทั้งหมดจะถูกออกแบบหรือจัดทำโดยหน่วยงานเทคโนโลยีสารสนเทศ (IT) บุคคลใดที่ต้องการเปลี่ยนค่าการติดตั้งเชื่อมต่อสายในการส่งข้อมูล ต้องมีการขออนุญาตจากหน่วยงาน IT ก่อนเริ่มต้นการทำงานนั้น ๆ
2. การเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องกับข้อมูลที่เป็นความลับของบริษัท ต้องมีการเข้ารหัสเสมอผู้ใช้งานในระบบเครือข่ายที่ไม่สิทธิ์ในการเข้าถึงระบบข้อมูลหรือเครือข่ายใด ๆ ต้องไม่ได้รับสิทธิ์ในการเข้าถึงนั้นหรือได้รับสิทธิ์มากกว่าที่มีอยู่โดยเด็ดขาด

สิทธิ์พิเศษในการติดต่อสื่อสาร

เครื่องคอมพิวเตอร์ทุกเครื่องไม่ว่าจะเป็นเครื่องที่ใช้งานประจำหรือว่าติดตั้งแบบชั่วคราว และมีการเชื่อมต่อไปยังเครือข่ายภายนอกได้เพื่อทำการเข้าถึงโดยมีสิทธิ์พิเศษ ต้องมีการควบคุมและเห็นชอบจากหน่วยงานความปลอดภัยข้อมูลก่อน ผู้ใช้งานทั่วไปไม่สามารถทำการค้นหาระบบหรือเครือข่ายได้โดยไม่รับอนุญาต

ข้อมูลที่ถูกต้องครบถ้วน

ข้อมูลจากอินเทอร์เน็ตต้องถูกแยกออกจากข้อมูลที่มาจากแหล่งอื่น และมีการตรวจสอบในไวรัสก่อนโดยซอฟต์แวร์ป้องกันไวรัสเวอร์ชันปัจจุบัน ผู้ใช้งานทั่วไปต้องไม่ลงซอฟต์แวร์ใดๆ บนเครื่องด้วยตัวเอง ห้ามเปิดไฟล์แนบมากับจดหมายอิเล็กทรอนิกส์หรืออีเมลถ้าหากจดหมายหรืออีเมลนั้นไม่ได้มาจากแหล่งที่เชื่อถือได้หรือบุคคลที่ที่รู้จัก

การรายงานเหตุการณ์

1. ถ้าข้อมูลสำคัญหรือข้อมูลลับของบริษัทเกิดสูญหาย ถูกเปิดเผยแก่บุคคลภายนอก หรือสงสัยว่าจะมีเหตุการณ์ลักษณะนี้เกิดขึ้น ต้องมีการแจ้งให้กับทางหัวหน้าหน่วยงานความปลอดภัยข้อมูลรับทราบโดยทันที ผู้ใช้งานทั่วไปที่ได้รับข้อมูลเกี่ยวกับช่องโหว่ของระบบที่ใช้งานอยู่ต้องทำการส่งต่อให้กับหน่วยงานความปลอดภัยข้อมูล
2. ผู้ใช้งานทั่วไป ต้องไม่ทำการทดสอบหรือทดลองการใช้งานวิธีการที่มีผลต่อระบบการใช้งานจริง ไม่ว่าจะภายในองค์กรหรือส่งผลต่อที่อื่นในอินเทอร์เน็ต ถ้าหากไม่ได้รับการเห็นชอบหรือ อนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

การสำรองข้อมูลและการนำข้อมูลกลับเข้าระบบ

1. ข้อมูลในระบบต่าง ๆ ควรมีการทำการสำรองข้อมูลลงบนสื่อบันทึกข้อมูลเป็นประจำ
2. ระบบการติดต่อสื่อสารหรือมีการใช้งานหลายๆ คน ทางผู้ดูแลระบบมีหน้าที่ทำการสำรองข้อมูลเป็นระยะอย่างต่อเนื่อง
3. เมื่อมีการร้องขอ หน่วยงานเทคโนโลยีสารสนเทศ (IT) ต้องให้ความช่วยเหลือในการติดตั้งฮาร์ดแวร์อุปกรณ์หรือซอฟต์แวร์ในการสำรองข้อมูล
4. การสำรองข้อมูล สำหรับข้อมูลที่เป็นความลับมาก ต้องมีการเก็บไว้ในที่ ๆ ปลอดภัยและถูกควบคุมการเข้าถึงอย่างเป็นระบบ

5. การสำรองข้อมูลลงอุปกรณ์จะต้องเก็บไว้ในที่ลับเฉพาะเพื่อจะนำมาใช้ใหม่เมื่อมีการนำข้อมูลกลับเข้าสู่ระบบ เมื่อเกิดเหตุการณ์ เช่น ระบบคอมพิวเตอร์ติดไวรัสและมีความเสียหายต้องมีการกู้ข้อมูล มีการติดไวรัสที่ฮาร์ดดิสก์ หรือเกิดปัญหาอื่น ๆ ที่เครื่องคอมพิวเตอร์ขึ้นเป็นต้น
6. มีการทำติดตามสถานะของการสำรองข้อมูลว่าสามารถสำรองข้อมูลได้อย่างสมบูรณ์ ทุกๆไตรมาส เพื่อให้มั่นใจว่าบริษัทจะสามารถนำสื่อบันทึกข้อมูลที่สำรองกลับมาใช้งานในกรณีฉุกเฉินได้
7. ต้องมีการจัดทำแผนสำรองฉุกเฉินไว้สำหรับแอปพลิเคชันต่าง ๆ ที่มีการจัดการเกี่ยวกับการใช้งานข้อมูลในระบบที่มีความสำคัญต่อธุรกิจ เจ้าของข้อมูลต้องแน่ใจว่าแผนที่จัดทำสามารถรองรับกับการใช้งานจริง มีการปรับปรุงแก้ไขให้ทันสมัยที่สุด และมีการทบทวนแผนอย่างต่อเนื่อง
8. พิจารณาให้มีการเข้ารหัสข้อมูลที่สำรองไว้ และจัดเก็บข้อมูลในลักษณะออฟไลน์

แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
ปัญหาจากการบุกรุกพื้นที่	กำหนดสิทธิ์การเข้าถึงพื้นที่ต่าง ๆ ของพนักงานและบุคคลภายนอก	ติดตั้ง Access Control และให้สิทธิ์การเข้าถึงพื้นที่ตามความเหมาะสม	ตรวจสอบการเข้าถึงพื้นที่ของพนักงานและบุคคลภายนอก	ทำการปรับตั้งค่าให้เหมาะสม, เพิ่ม – ลบ ข้อมูลของพนักงานใหม่ และพนักงานที่พ้นสภาพ
ปัญหาจากการกระทำความผิดตามพรบ. คอมพิวเตอร์	ทำการบันทึกการเข้าใช้งานระบบ (Log) ตาม พรบ. คอมพิวเตอร์	จัดเก็บข้อมูลการใช้งานระบบไม่น้อยกว่าเก้าสิบวันตาม พรบ.คอมพิวเตอร์	ตรวจสอบการบันทึกข้อมูลในอุปกรณ์บันทึกข้อมูล พร้อมประมาณการบันทึกข้อมูลตามการใช้งานระบบ	เพื่อสื่อบันทึกข้อมูล กรณีพื้นที่บันทึกข้อมูลไม่เพียงพอต่อจำนวนวันที่ต้องบันทึก
ปัญหาจากการติดต่อสื่อสารจากระบบเทคโนโลยีสารสนเทศ	พนักงานใช้งานระบบตามชื่อบัญชีของตน	พนักงานเข้าใช้งานระบบของตนตามที่ได้ส่งมอบให้	ตรวจสอบระบบการทำงาน จาก Log ระบบที่ได้บันทึกไว้	หากไม่สามารถใช้งานได้ สามารถติดต่อเจ้าหน้าที่ไอทีเพื่อดำเนินการแก้ไขปัญหา
ปัญหาจากการกำหนดสิทธิ์การใช้งาน	พนักงานต้องใช้งานระบบด้วยชื่อบัญชีของพนักงานเท่านั้น	พนักงานเข้าใช้ระบบด้วยชื่อบัญชีของตน	ตรวจสอบระบบการทำงาน จาก Log ระบบที่ได้บันทึกไว้	จัดทำระบบเฝ้าระวังการใช้งาน ชื่อบัญชีของพนักงานแบบไม่พึงประสงค์
ปัญหาจากการใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ตรวจสอบการใช้งานซอฟต์แวร์ขององค์กร	จัดหาซอฟต์แวร์ที่ใช้งานภายในองค์กร จัดซื้อซอฟต์แวร์ที่จำเป็นและจัดหาซอฟต์แวร์โอเพ่นซอร์สเพื่อใช้งานทดแทน	ตรวจสอบการใช้งานซอฟต์แวร์ในเครื่องพนักงาน	รับแจ้งความต้องการใช้งานซอฟต์แวร์เพิ่มเติมพร้อมตรวจสอบจำนวนอุปกรณ์ที่ใช้งานภายในสำนักงาน
ปัญหาจากไวรัสคอมพิวเตอร์และ	ป้องกันไวรัสและการโจมตีทางไซเบอร์ ผ่าน	ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องคอมพิวเตอร์ที่ใช้งานและ	ตั้งค่าแจ้งเตือนเมื่อพบไวรัส หรือการโจมตีต่าง ๆ มายังเจ้าหน้าที่ไอที	อัพเดตรายชื่อไวรัสและการโจมตีต่าง ๆ ในระบบที่ใช้งานติดตามข่าวสารและทำ

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
การโจมตีทางไซเบอร์	ระบบเครือข่ายและอินเตอร์เน็ต	เปิดความสามารถป้องกันไวรัสและป้องกันการโจมตีทางไซเบอร์ที่ไฟล์วอล		การตรวจสอบปรับปรุงระบบ และปิดช่องโหว่ต่าง ๆ ที่มีประกาศออกมาก
ปัญหาจากการเข้าถึงข้อมูลจากบุคคลที่ไม่มีสิทธิ์จากภายนอกองค์กร	จัดทำระบบเครือข่ายส่วนตัวแบบเสมือน (VPN) ให้ใช้งาน กรณีต้องใช้งานระบบจากภายนอกสำนักงาน	พนักงานใช้งานระบบดังกล่าวในการดำเนินการ	ตรวจสอบ Log การใช้งาน ตรวจสอบหาความผิดปกติในการใช้งาน และติดตั้งระบบแจ้งเตือน เมื่อมีการใช้งานแบบผิดปกติ	ตรวจสอบการใช้งาน ว่าเพียงพอกับความต้องการหรือไม่
ปัญหาจากการกระแสไฟฟ้า	มีกระแสไฟฟ้าจ่ายให้ระบบอย่างต่อเนื่อง	ทำการติดตั้งระบบสำรองไฟฟ้าในระบบที่ให้บริการ	ทดสอบการทำงานผ่านระบบที่มีในเครื่องสำรองไฟฟ้า	ตรวจสอบการทำงานว่าสามารถสำรองไฟฟ้าได้ เป็นระยะเวลาที่กำหนดหรือไม่ หากมีการทำงานไม่ตรงกับข้อกำหนดให้ดำเนินการปรับปรุง เช่นลดการใช้กระแสไฟฟ้า เพิ่มระบบสำรองไฟฟ้า
ปัญหาจากระบบอินเตอร์เน็ต	ระบบสามารถใช้งานอินเตอร์เน็ตได้อย่างต่อเนื่อง	ติดตั้งอินเตอร์เน็ตเพื่อให้ระบบใช้งาน	จัดทำระบบตรวจสอบการทำงานของอินเตอร์เน็ต	ทำระบบตรวจจับการทำงานของอินเตอร์เน็ต, ขอติดตั้งอินเตอร์สำรอง ป้องกันปัญหาผู้ให้บริการไม่สามารถให้บริการ ได้
ปัญหาจากอุปกรณ์ระบบเครือข่ายและเครื่องแม่ข่าย	อุปกรณ์พร้อมใช้งานเสมอ	เมื่อเกิดปัญหาให้ดำเนินการแก้ไขให้ระบบกลับมาใช้งานได้	ทำการตรวจสอบการทำงานทุกวันว่า ระบบพร้อมทำงาน ตรวจสอบการทำงาน หลังจากทำการแก้ไขปัญหา	ทำการซื้อการสนับสนุนจากผู้ผลิตและตัวแทนจำหน่าย ปรับเปลี่ยนอุปกรณ์ตามอายุการใช้งาน, วางแผนป้องกันสาเหตุที่พบปัญหา
ปัญหาข้อมูลสูญหายจากระบบ	พนักงานสามารถใช้งานระบบและข้อมูลได้	เมื่อได้รับแจ้ง เจ้าหน้าที่ไอที จะทำการตรวจสอบและกู้คืนระบบตามที่ได้รับแจ้ง	ทำการตรวจสอบระบบสำรองข้อมูล, ทำการบันทึกผลข้อมูล และจัดเก็บสื่อบันทึกข้อมูลพร้อมทำป้ายกำกับอย่างเหมาะสม	เพิ่มสื่อบันทึกข้อมูลตามความเหมาะสม
ปัญหาจากซอฟต์แวร์และโปรแกรมที่ใช้งาน	ระบบสามารถให้บริการต่าง ๆ ได้	เมื่อรับแจ้งปัญหา เจ้าหน้าที่ไอทีทำการตรวจสอบระบบและดำเนินการแก้ไขปัญหา	ทำการตรวจสอบการทำงานของระบบ, ซอฟต์แวร์ และโปรแกรมที่ใช้งานพร้อมบันทึกผล	ทำการตรวจสอบ Patch, และทำการ Update ที่เหมาะสมกับระบบ

เหตุการณ์	การวางแผน	การดำเนินการ	การตรวจสอบ	การปรับปรุงเพิ่มเติม
ปัญหาจากการไม่สามารถเข้าถึงพื้นที่สำนักงาน	เมื่อพนักงานไม่สามารถเข้าถึงพื้นที่สำนักงานเพื่อปฏิบัติงานได้	พนักงานสามารถเข้าถึงระบบไอที จาก Internet ผ่าน VPN	ตรวจสอบว่า VPN พร้อมใช้งาน	ขยายช่องสัญญาณให้เหมาะสมตามการใช้งาน
ปัญหาจากอัคคีภัย	มีระบบแจ้งเตือนอัคคีภัย และระบบดับเพลิงในห้องศูนย์ข้อมูลเบื้องต้น	เมื่อพบเหตุผู้ประสบเหตุสามารถแจ้ง เจ้าหน้าที่ไอที เพื่อเปิดห้อง และดำเนินการดับเพลิงด้วยอุปกรณ์ที่จัดเตรียมไว้ หากสามารถดับเพลิงได้ให้ทำการแจ้งเจ้าหน้าที่ที่เกี่ยวข้อง หากไม่สามารถดับเพลิงได้ ให้ทำการอพยพตามแผนดับเพลิง ของอาคาร	ทำการตรวจสอบผลกระทบจากเพลิงไหม้ ว่าระบบสามารถทำงานต่อได้หรือไม่ ถ้าสามารถดำเนินการต่อได้ ให้ทำบันทึกข้อมูล ก่อนเปิดระบบ และตรวจสอบการทำงานของระบบ หากไม่สามารถเปิดระบบที่ประสบเหตุได้ ให้ทำการจัดหาอุปกรณ์เพื่อทำการกู้คืนระบบ	ติดตั้งอุปกรณ์ป้องกันเพลิงไหม้ที่ทำงานแบบอัตโนมัติ, ทำการสำรองข้อมูลและจัดเก็บสื่อบันทึกข้อมูลในสถานที่ อื่น, จัดให้พนักงานไอทีที่เกี่ยวข้องอบรมการใช้งาน เครื่องดับเพลิงสำหรับศูนย์คอมพิวเตอร์
ปัญหาจากความไม่สงบเรียบร้อยในบ้านเมือง	ระบบไอทีสามารถทำงานได้	ให้พนักงานใช้งานระบบผ่าน VPN	ตรวจสอบการใช้งานและช่องสัญญาณให้เพียงพอต่อการใช้งาน	ขยายช่องสัญญาณหากมีการใช้งานปริมาณสูง หรือย้ายขึ้นระบบ Cloud หรือทำศูนย์ข้อมูลสำรอง หากมีปัญหาไม่สามารถ ใช้บริการศูนย์ข้อมูลหลักได้
ปัญหาจากภัยพิบัติเป็นผลให้ระบบเดิมไม่สามารถให้บริการได้	ระบบไอทีสามารถทำงานได้	ทำการจัดหาอุปกรณ์และโครงสร้างพื้นฐานที่จำเป็นสำหรับระบบทั้งหมด และดำเนินการ กู้ข้อมูลจากสื่อบันทึกข้อมูลจากแหล่งที่จัดเก็บ สื่อข้อมูลสำรอง เมื่อดำเนินการแล้วเสร็จจะทำการตรวจสอบการทำงานของระบบตามการตรวจสอบประจำวัน	ตรวจสอบการใช้งานว่าสามารถให้บริการได้ตามปกติ	ในการจัดหาโครงสร้างพื้นฐานสำหรับระบบทั้งหมด อาจใช้เวลานาน ซึ่งอาจนำระบบ Cloud มาร่วมในการกู้คืนระบบได้

การจัดการกับการเปลี่ยนแปลง (CHANGE MANAGEMENT)

1. ระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารของบริษัทที่ใช้สำหรับการดำเนินการทางธุรกิจต้องมีเอกสารซึ่งบอกถึงขั้นตอนในจัดการกับการเปลี่ยนแปลงในระบบอย่างชัดเจน เพื่อให้แน่ใจว่าบุคคลที่กระทำการเปลี่ยนแปลงข้อมูลต่าง ๆ ในระบบเป็นผู้ที่ได้อนุญาตและมีสิทธิ์ในการเปลี่ยนแปลงนั้น ๆ จริง
2. ต้องมีการปฏิบัติตามระเบียบขั้นตอนของการจัดการที่กำหนดไว้ทุกครั้ง ในกรณีที่มีการเปลี่ยนแปลงค่าต่าง ๆ ที่มีผลกระทบกับระบบการทำงานจริง อุปกรณ์ การเชื่อมต่อ หรือขั้นตอนปฏิบัติงาน
3. นโยบายนี้รวมไปถึงคอมพิวเตอร์ที่ใช้ทำงานในระบบปฏิบัติงานจริงและระบบการใช้งานที่เข้าถึงได้จากพนักงานหลายคนด้วย

การพัฒนาและปรับปรุงรักษาระบบ

1. การพัฒนาและการปรับปรุงรักษาซอฟต์แวร์สำหรับการใช้งานจริงในระบบโดยพนักงานของบริษัทต้องปฏิบัติตามนโยบายของแผนกเทคโนโลยีสารสนเทศ มาตรฐาน ขั้นตอนและระเบียบต่าง ๆ ของบริษัท
2. ระเบียบต่าง ๆ ที่กล่าวถึงนี้รวมไปถึงการทดสอบ การฝึกอบบรม และเอกสารอ้างอิงที่จัดทำไว้
3. การเปลี่ยนแปลงไฟล์หรือซอฟต์แวร์ต่าง ๆ ก็ต้องปฏิบัติตามระเบียบข้อกำหนดของการควบคุมการจัดการการเปลี่ยนแปลงระบบด้วย (Change management)

การจัดการเกี่ยวกับใบอนุญาตซอฟต์แวร์

1. ผู้บริหารต้องต่อรองข้อตกลงอย่างเหมาะสมกับทางผู้ให้บริการซอฟต์แวร์โดยคำนึงถึงความจำเป็นในการใช้ใบอนุญาตซอฟต์แวร์หรือ License เพิ่มเติม
2. จะมีการซื้อซอฟต์แวร์ที่มีความจำเป็นต่อการใช้งานจริงในบริษัท

การเข้าถึงข้อมูลที่เป็นความลับโดยสิทธิ์อ่านได้อย่างเดียว

ผู้ใช้งานที่มีสิทธิ์ในการเข้าถึงข้อมูลที่เป็นความลับโดยการอ่านได้อย่างเดียว ต้องได้รับอนุญาตในการเข้าถึงเพียงข้อมูลระดับนี้หรือน้อยกว่าระดับนี้เท่านั้น

การเข้าถึงข้อมูลที่เป็นความลับโดยมีสิทธิ์การแก้ไขได้

ผู้ใช้งานต้องไม่ทำการเคลื่อนย้ายข้อมูลที่อยู่ในระดับนี้ไปยังระดับที่อยู่น้อยกว่า เว้นแต่จะมีการทำการยกเลิกข้อมูลชนิดนี้ออกจากระดับข้อมูลนี้ ตามขั้นตอนที่ถูกต้อง

การจัดการบัญชีผู้ใช้งาน

พนักงานแต่ละคนจะได้รับบัญชีผู้ใช้งาน (User Id) ของตัวเองซึ่งจะเป็นข้อมูลการใช้งานของพนักงานคนนั้น ๆ โดยเฉพาะ ผู้จัดการต้องมีการแจ้งให้หน่วยงานที่รับผิดชอบในการตั้งค่าบัญชีผู้ใช้งาน เมื่อพนักงานคนนั้นมีการเปลี่ยนแปลงในเรื่องของหน้าที่การทำงาน สิทธิ์ในการเข้าถึง และอื่น ๆ ที่เกี่ยวข้องกับการทำงานของพนักงานทันที บัญชีผู้ใช้งานต้องไม่สามารถใช้งานได้อีกต่อไปเมื่อเจ้าของบัญชีผู้ใช้งานนั้นลาออกจากบริษัทหรือไม่มีสิทธิ์ในการเข้าถึงงานหรือระบบที่เกี่ยวข้องกับบัญชีการใช้งานนั้นในบริษัทอีกต่อไป

การจัดการสิทธิพิเศษ

สิทธิพิเศษในเรื่องเกี่ยวกับคอมพิวเตอร์และระบบการติดต่อสื่อสารของผู้ใช้งาน ระบบ โปรแกรมทั้งหมด ต้องถูกกำหนดให้ขึ้นอยู่กับความจำเป็นในการใช้งาน ในกรณีที่มีการร้องขอพิเศษ จะขึ้นอยู่กับความรับผิดชอบโดยตรงที่เกี่ยวข้องกับการบริหารจัดการระบบหรือความปลอดภัยข้อมูล และต้องทำการยกเลิกทันที เมื่อไม่ได้มีการใช้งานแล้ว

การควบคุมการเข้าถึงโดยใช้รหัสผ่าน

ระบบที่มีขนาดเล็ก แต่มีการจัดการเกี่ยวกับข้อมูลที่เป็นความลับหรือข้อมูลสำคัญ ต้องมีการกำหนดให้ใช้ระบบการเข้าถึงโดยใช้รหัสผ่าน

ซอฟต์แวร์อันตราย

ซอฟต์แวร์ตรวจสอบไวรัส (Virus Detection Software)

1. ผู้ใช้งานระบบคอมพิวเตอร์ไม่ควรจะยกเลิกหรือปิดขั้นตอนการอัพเดทเวอร์ชันไวรัสที่ทำงานขึ้นเองโดยอัตโนมัติ
2. ไฟล์ของระบบทุกไฟล์ควรจะมีการสแกนหรือตรวจสอบโดยซอฟต์แวร์ที่ใช้ตรวจสอบไวรัส
3. ต้องมีการสแกนไวรัสก่อนที่จะเปิดไฟล์ใหม่ๆ หรือก่อนที่จะทำการเปิดหรือติดตั้งซอฟต์แวร์ตัวใหม่ก่อน

ความปลอดภัยของระบบเครือข่าย

การเชื่อมต่อระบบเครือข่ายภายใน

1. คอมพิวเตอร์ทุกเครื่องที่ทำหน้าที่เก็บข้อมูลที่เป็นความลับหรือมีการเชื่อมต่อกับระบบคอมพิวเตอร์เครือข่ายของบริษัทเพื่อใช้งานเป็นประจำ หรือชั่วคราวต้องได้รับการอนุญาตในการเข้าถึงระบบจากหน่วยงานความปลอดภัยข้อมูลก่อน
2. ระบบการจัดการประมวลผลข้อมูลทุกชนิดต้องติดตั้งรหัสผ่านหรือมีการล็อคหน้าจอหลังจากที่ไม่มีการใช้งานอัตโนมัติภายในระยะเวลาที่กำหนดไว้ และเมื่อต้องการใช้งานอีกครั้ง ก็ต้องมีการร้องขอให้ใส่รหัสผ่าน
3. ระบบที่ใช้งานหลายคนต้องใช้วิธีการปิดการเชื่อมต่ออัตโนมัติเมื่อไม่มีการใช้งานของผู้ใช้งานเกิดขึ้นในระยะเวลาหนึ่งหรือภายในระยะเวลาที่กำหนดไว้

การเชื่อมต่อระบบเครือข่ายภายนอก

1. การเชื่อมต่อระบบจากภายนอกเข้าสู่ระบบข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการป้องกันโดยระบบการเข้าถึงโดยการใช้รหัสผ่านแบบเปลี่ยนแปลงได้ (dynamic password) หรือใช้รหัสผ่านแบบตรวจสอบความเป็นตัวตนจากจุดเดียว (Single sign-on user and password) การใช้งานรหัสผ่านแบบเปลี่ยนแปลงได้ในแต่ละครั้งที่มีการใช้งานสามารถป้องกันการขโมยรหัสผ่านได้
2. พนักงานบริษัทไม่ควรจะเชื่อมต่อหรือสร้างการเชื่อมต่อออกไปยังเครือข่ายภายนอกหรืออินเทอร์เน็ตเอง โดยใช้ระบบขององค์กร โดยไม่ได้รับอนุญาตจากหน่วยงานความปลอดภัยข้อมูลก่อน

การเปลี่ยนแปลงระบบเครือข่าย

1. การเปลี่ยนแปลงระบบคอมพิวเตอร์ของบริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการบันทึกลงในแบบฟอร์มการขอเปลี่ยนแปลง (change request form) และต้องได้รับการอนุมัติจากผู้มีอำนาจในขั้นตอนการควบคุมการเปลี่ยนแปลงนั้น ยกเว้นได้ในกรณีฉุกเฉินเท่านั้น
2. การเปลี่ยนแปลงต่าง ๆ ที่มีผลมายังระบบเครือข่ายภายในต้องมีการแจ้งให้กับผู้มีอำนาจหรือผู้รับผิดชอบในส่วนงานเทคโนโลยีสารสนเทศรับทราบก่อน
3. ขั้นตอนนี้สามารถลดความเสี่ยงที่เกิดจากผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลและการเปลี่ยนแปลงนี้อาจจะทำ ให้เกิดผลร้ายแรงได้จากผู้ที่รู้เท่าไม่ถึงการณ์ถึงแม้ว่าจะมีสิทธิ์ในแผนกเทคโนโลยีสารสนเทศได้
4. ขั้นตอนนี้กำหนดใช้กับพนักงานบริษัทสกาย ไอซีทีและกลุ่มบริษัทในเครือ และรวมไปถึงผู้ที่ให้บริการด้วย

การทำงานทางไกล

1. พนักงานในบางหน่วยงานสามารถมีสิทธิ์ในการทำงานจากที่บ้านได้
2. การอนุญาตเพื่อให้ทำงานจากทางไกลได้นั้น ส่วนหนึ่งขึ้นอยู่กับนโยบายและมาตรฐานความปลอดภัยข้อมูล

การจัดการความเสี่ยง

เพื่อให้การปฏิบัติงานของระบบคอมพิวเตอร์และระบบเครือข่ายเป็นไปอย่างต่อเนื่องด้วยดี บริษัท สกาย ไอซีที จำกัด (มหาชน) ต้องมีการจัดทำแผนการดำเนินงานทางธุรกิจให้ต่อเนื่อง (Business continuity plan) ซึ่งประกอบไปด้วย:

1. การประเมินความเสี่ยงทางธุรกิจ
2. ลักษณะของการบริหารความเสี่ยง
3. การระบุความเสี่ยงที่จะเกิดขึ้น
4. การวัดค่าความเสี่ยง
5. แผนการรับมือกับความเสี่ยงที่จะเกิดขึ้น
6. ความเสี่ยงที่สามารถยอมรับได้
7. การเลือกวิธีหรือเครื่องมือป้องกัน
8. การพิจารณาผลการประเมินความเสี่ยง

แผนการดำเนินงานทางธุรกิจให้ต่อเนื่อง (BCP)

องค์กรต้องมีการตั้งทีมงานเพื่อทำแผนการจัดการเกี่ยวกับการบริหารความเสี่ยงและอบรมให้ความรู้แก่ผู้ใช้งานถึงเรื่องแผนการดำเนินงานทางธุรกิจให้ต่อเนื่องเป็นประจำทุกปี รวมถึงการปรับปรุงแผนการและต้องมีการอัพเดทให้ใหม่เข้ากับสถานการณ์ขององค์กรปัจจุบัน และทำการอัพเดทในความเป็นไปได้ทุกเหตุการณ์ที่อาจจะเกิดขึ้น ซึ่งจะต้องประกอบไปด้วยลักษณะอาการต่าง ๆ สาเหตุที่ทำให้เกิด และวิธีการแก้ไข

การบันทึกการจราจรข้อมูลทางอินเทอร์เน็ต

อ้างถึงมาตรฐานการเก็บบันทึกการจราจรข้อมูลหรือล็อก (Log) กำหนดโดยกระทรวงเทคโนโลยีสารสนเทศของประเทศไทยปี 2550 ซึ่งมีชนิดของข้อมูล หรือล็อกที่ต้องได้รับการบันทึกและเก็บไว้ดังนี้

1. ล็อกของระบบเครือข่าย
   - ข้อมูลการเข้าถึงระบบระบุถึงบุคคลที่สามารถเข้าถึงและสิทธิ์ในการเข้าถึงระบบเครือข่าย
   - ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
   - ข้อมูลของบัญชีผู้ใช้งานระบุตัวตนผู้ใช้งาน
   - ข้อมูลเลขหมายหรือ IP Address ที่กำหนดให้เครื่องลูกข่าย
   - ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา
2. ล็อกของการใช้งานจดหมายอิเล็กทรอนิกส์หรืออีเมล ทางบริษัท สกาย ไอซีที จำกัด (มหาชน) ใช้บริการ จดหมายอิเล็กทรอนิกส์ Microsoft Exchange / Microsoft Office 365 suite อาจจะมีข้อมูลหลายๆ ข้อนี้
   - ข้อมูลหมายเลขของข้อความที่ระบุในอีเมล (Message ID)
   - ข้อมูลชื่อที่อยู่อีเมลของผู้ส่ง
   - ข้อมูลชื่อที่อยู่อีเมลของผู้รับ
   - ข้อมูลที่บ่งบอกสถานะของอีเมล เช่น ส่งล่าช้า ส่งสำเร็จ ปฏิเสธการส่ง หรือส่งคืนผู้ส่ง เป็นต้น
   - ข้อมูลเลขหมาย หรือ IP address ที่กำหนดให้เครื่องลูกข่าย
   - ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
   - ชุดข้อมูลเลขหมาย หรือ IP address ของเครื่องผู้ส่งอีเมล
   - บัญชีชื่อผู้ใช้งาน
   - ข้อมูลที่มีการบันทึกการเข้า ออก ของอีเมล ผ่านโปรแกรมการจัดการจากเครื่องของสมาชิกหรือการเข้าถึงเพื่อเรียกข้อมูลอีเมลไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลอีเมลที่ดึงไปนั้นไว้ที่เครื่องให้บริการหรือเครื่องเซิร์ฟเวอร์ (POP3 or IMAP4 log)
3. ล็อกโอนไฟล์หรือข้อมูล
   - ข้อมูลทุกอย่างเมื่อมีการเข้าถึงเครื่องให้บริการโอนไฟล์ข้อมูล
   - ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
   - ข้อมูลหมายเลขของเครื่องคอมพิวเตอร์ที่เข้ามาทำการเชื่อมต่ออยู่ในขณะนั้น
   - บัญชีชื่อผู้ใช้งาน
   - ข้อมูลตำแหน่งและชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป
   - ข้อมูลการเข้าถึง แก้ไข หรือเปลี่ยนแปลงข้อมูล รวมถึงการเปลี่ยนแปลงสิทธิของผู้ใช้งาน

4. ล็อกการเข้าถึงอินเทอร์เน็ต
   - ข้อมูลเกี่ยวกับวันและเวลาในการติดต่อระหว่างเครื่องลูกข่ายและเครื่องเซิร์ฟเวอร์
   - ข้อมูลหมายเลขหรือ IP address ของเครื่องที่ทำการเชื่อมต่อไปยังเครื่องให้บริการหรือเครื่องเซิร์ฟเวอร์และคำสั่งการใช้งาน

ข้อปฏิบัติและข้อบังคับตามกฎหมาย

บริษัท สกาย ไอซีที จำกัด (มหาชน) มีการจัดทำการตรวจสอบความปลอดภัยข้อมูลเพื่อให้ถูกต้องและตรงกับนโยบาย ระเบียบและกฎหมายอย่างต่อเนื่อง

การปฏิบัติตามนโยบายและระเบียบ

พนักงานทุกคนต้องปฏิบัติตามนโยบายความปลอดภัยข้อมูลและเอกสารที่เกี่ยวข้องกับนโยบายนี้ รวมถึงนโยบายอื่นๆที่เกี่ยวข้องอย่างเคร่งครัด เช่น นโยบายการคุ้มครองข้อมูลส่วนบุคคล พนักงานท่านใดที่ละเลย หรือมีเจตนาที่จะไม่ปฏิบัติตาม ถือว่ามีการละเมิดนโยบายดังกล่าว จะได้รับบทลงโทษหรืออาจจะร้ายแรงถึงขั้นไล่ออก

การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ

นโยบายความปลอดภัยข้อมูลจะต้องเป็นไปตามข้อบังคับทางกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กฎหมายที่เกี่ยวกับการป้องกันข้อมูล การเข้าถึงข้อมูล การป้องกันข้อมูลส่วนตัว และเอกสารอิเล็กทรอนิกส์ต่าง ๆ เป็นต้น

ตามระเบียบข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นถือว่าบริษัท สกาย ไอซีที จำกัด (มหาชน) เป็นผู้ให้บริการเข้าถึงอินเทอร์เน็ต ซึ่งต้องมีการบันทึกและเก็บการบันทึกข้อมูลจราจรทางอินเทอร์เน็ตทั้งหมดตามวันและเวลาที่เข้าถึง ย้อนหลังอย่างน้อย 90 หรือมากกว่านั้น

ระเบียบและบทลงโทษ

1. การกระทำที่สงสัยว่าจะละเมิดนโยบายการรักษาความปลอดภัย (การเจาะข้อมูล, การทำลายข้อมูลของไวรัสคอมพิวเตอร์) หรือสงสัยว่ามีการล่วงละเมิดหรือแทรกแซงระบบข้อมูล ต้องแจ้งให้กับผู้บริหาร และเจ้าหน้าที่รักษาความปลอดภัยข้อมูลทราบทันที
2. การกระทำที่สงสัยว่าจะละเมิดข้อมูลส่วนบุคคล ต้องดำเนินการแจ้งให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทันทีโดยอ้างอิงจาก "**นโยบายการคุ้มครองข้อมูลส่วนบุคคล**"
3. การละเมิดหรือการไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยของข้อมูล มีบทลงโทษต่อผู้ละเมิดอย่างร้ายแรงระเบียบการลงโทษมีความรุนแรงขึ้นอยู่กับการกระทำ และสามารถรุนแรงถึงขั้นไล่ออก
4. การทำตามระเบียบของพนักงานทั้งหมดที่อยู่ภายใต้การดูแลของหัวหน้าแผนกหรือผู้มีระดับที่สูงกว่า เมื่อพนักงานทำผิดหรือละเมิดกฎหัวหน้าแผนกหรือผู้มีระดับที่สูงกว่าจะเป็นผู้พิจารณาลงโทษ

5. การกระทำที่ถือว่าเป็นการละเมิดกฎมีดังนี้

5.1. การเปลี่ยนแปลงแก้ไขข้อมูลภายในระบบโดยไม่ได้รับอนุญาตจากผู้มีอำนาจหรือหัวหน้างานก่อน

5.2. การปลอมแปลง ขโมย ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานในระบบแอปพลิเคชันใด ๆ โดยตั้งใจหรือไม่ตั้งใจก็ตาม

5.3. การใช้บัญชีผู้ใช้งานและรหัสผ่านของผู้อื่นในการเข้าใช้งานระบบคอมพิวเตอร์เพื่ออ่าน คัดลอกหรือทำสำเนา เปลี่ยนแปลงหรือลบข้อมูลไม่ว่าจะด้วยเหตุผลใด ๆ ก็ตาม

5.4. การละเลยและอนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้งานและรหัสผ่านของตัวเองในการเข้าใช้งานระบบคอมพิวเตอร์รวมถึงให้ใช้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์นั้น ๆ ด้วย

5.5. ทำการพยายามเปิดเผย ขาย และกระจายข้อมูลของบริษัท สกาย ไอซีที จำกัด (มหาชน)

5.6. การพยายามเข้าใช้งานระบบและแอพลิเคชั่นใด ๆ โดยไม่มีสิทธิ์ในการใช้งาน

5.7. การติดตั้ง ตรวจสอบ เฝ้าดู และใช้เครื่องมือหรือซอฟต์แวร์ในการเจาะข้อมูล (hacking tools) หรือโปรแกรมที่เกี่ยวกับตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์ ยกเว้นผู้ที่มีหน้าที่รับผิดชอบในด้านในการทำการดังกล่าวเท่านั้น

5.8. ติดตั้งและทำการเปลี่ยนแปลงหมายเลขของเครื่องคอมพิวเตอร์ (IP address) โดยไม่ได้รับอนุญาตจากหน่วยงานเทคโนโลยีสารสนเทศ (IT) ก่อน

5.9. การเปลี่ยนแปลง โอนย้าย หรือติดตั้ง ส่วนใดส่วนหนึ่งในระบบคอมพิวเตอร์โดยไม่ได้รับการอนุญาตจากแผนก IT ก่อน

5.10. การร่วมมือกับบุคคลภายนอกเพื่อให้เข้ามาใช้งานระบบคอมพิวเตอร์หรือโปรแกรมแอปพลิเคชันใด ๆ หรือทำลายการรักษาความปลอดภัยของข้อมูลหรือระบบของบริษัท สกาย ไอซีที จำกัด (มหาชน)

6. บทลงโทษการฝ่าฝืนและละเลย

5.5. การกล่าวตักเตือน

5.6. ออกจดหมายเตือน

5.7. ได้รับการพักงานชั่วคราว

5.8. พ้นสภาพจากการเป็นพนักงานของบริษัท

บริษัทฯ จะพิจารณาและใช้ความละเอียดรอบคอบในการลงโทษพนักงานที่ทำผิดหรือละเมิดนโยบาย

บทสรุป

บริษัท สกาย ไอซีที จำกัด (มหาชน) จำเป็นต้องมีการพัฒนานโยบาย ระเบียบขั้นตอน ข้อแนะนำ และมาตรฐานต่าง ๆ ขึ้นมา เพื่อให้การสนับสนุนการทำงานในส่วนนโยบายความปลอดภัยข้อมูลนี้ ซึ่งมีการประกาศใช้อย่างเป็นทางการให้ได้รับทราบภายในบริษัท คู่มือของนโยบายการรักษาความปลอดภัย สามารถใช้อ้างอิงถึงมาตรฐานหรือนโยบายย่อยที่ใช้ควบคุมระบบต่าง ๆ ภายในองค์กรและมีการอัพเดทปรับปรุงอย่างต่อเนื่อง

บริษัทฯ จึงขอแจ้งนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อเป็นกรอบและแนวทางในการปฏิบัติ อนึ่ง ให้ยกเลิกข้อความในประกาศและข้อบังคับการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่มีอยู่เดิมทั้งหมด และให้ยึดถือประกาศฉบับนี้แทน ให้มีผลย้อนหลังโดยเริ่มมีผลตั้งแต่วันที่ 1 ธันวาคม 2564 เป็นต้นไป

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 3 ธันวาคม พ.ศ. 2564

.....

(นายสิทธิเดช มัยลาภ)
ประธานเจ้าหน้าที่บริหาร
บริษัท สกาย ไอซีที จำกัด (มหาชน)