นโยบายความมั่นคงปลอดภัยสารสนเทศ

ของ
บริษัท น้ำตาลขอนแก่น จำกัด (มหาชน) และ
บริษัทในกลุ่ม

นโยบายความมั่นคงปลอดภัยสารสนเทศ

สาระสำคัญในนโยบายความมั่นคงปลอดภัยสารสนเทศฉบับนี้ถูกกำหนดให้เป็นแม่บทในการปฏิบัติเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทน้ำตาลในกลุ่ม เค.เอส.แอล. อันประกอบไปด้วย

1. บริษัท น้ำตาลขอนแก่น จำกัด (มหาชน)
2. บริษัท น้ำตาลท่ามะกา จำกัด
3. บริษัท โรงงานน้ำตาลนิวกรุงไทย จำกัด
4. บริษัท น้ำตาลนิวกว้างสุ้นหลี จำกัด
5. บริษัท น้ำตาลสะหวันนะเขต จำกัด
6. บริษัท น้ำตาลเกาะกง จำกัด
7. บริษัท เกาะกงการเกษตร จำกัด
8. บริษัท โรงงานไฟฟ้าน้ำตาลขอนแก่น จำกัด
9. บริษัท เคเอสแอล อะโกร แอนด์เทรดดิ้ง จำกัด
10. บริษัท เคเอสแอล เรียลเอสเทต จำกัด
11. บริษัท เคแอสแอล เอ็กซ์ปอร์ต เทรดดิ้ง จำกัด
12. บริษัท เคเอสแอล แมททีเรียล ซัพพลายส์ จำกัด
13. บริษัท ราชาชูรส จำกัด
14. บริษัท ราชาเซรามิค จำกัด
15. บริษัท ราชาปอร์ซเลน จำกัด
16. บริษัท ราชาโปรดักส์ จำกัด
17. บริษัท เซ็งเพรส จำกัด
18. หจก. แม่สอดเซรามิค
19. บริษัท ราชาโซล่าร์แมททีเรียล จำกัด

เพื่อให้สามารถดำเนินงานได้อย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย สามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ และการถูกภัยคุกคามต่างๆ โดยมีหลักการดังต่อไปนี้

1. การกำหนดขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อ้างอิงข้อกำหนด กฎหมาย และวิธีปฏิบัติที่ดีต่อไปนี้
   1) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544
   2) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551
   3) หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.2550
   4) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2553

5) หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ พ.ศ.2553
6) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
7) มาตรฐาน ISO/IEC 27001

2. นโยบายนี้จะต้องทำการเผยแพร่แก่เจ้าหน้าที่ที่เกี่ยวข้องทุกระดับได้รับทราบ
3. นโยบายนี้ต้องมีการดำเนินการทบทวนตามระยะเวลา 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

นอกจากนี้ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทอนิกส์ พ.ศ. 2553 ได้ประกาศให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือบริษัท หรือส่วนงานหรือบริษัทที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ต้องกระทำตามวิธีการแบบปลอดภัย โดยให้ถือว่าธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวได้กระทำตามวิธีที่เชื่อถือได้ตามมาตรา 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งผู้กระทำต้องคำนึงถึงหลักการพื้นฐาน ดังนี้

1. การรักษาความลับ (Confidentiality)
2. การรักษาความครบถ้วน (Integrity)
3. การรักษาสภาพพร้อมใช้งาน (Available)

รวมทั้งการปฏิบัติตามนโยบายและแนวปฏิบัติการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทฯ

องค์ประกอบของนโยบาย

บทนิยาม

“การรักษาความมั่นคงปลอดภัย”
หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

“ความมั่นคงปลอดภัยด้านสารสนเทศ”
หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (reliability)

“ข้อมูล”
หมายถึง ข้อมูลและข้อมูลสารสนเทศทั้งที่อยู่ในรูปเอกสารและข้อเท็จจริงที่อยู่ในรูปแบบต่างๆ เช่น ข้อมูลที่อยู่ในแบบฟอร์มของบริษัท รวมถึงที่อยู่ในระบบสารสนเทศ เครือข่าย อุปกรณ์คอมพิวเตอร์ หรือสื่อในการจัดเก็บข้อมูลของบริษัท ไม่ว่าข้อมูลเหล่านี้จะอยู่ในรูปแบบใด ๆ การอ้างถึงข้อมูลตามข้อกำหนดนี้ จะมีความหมายรวมถึงข้อมูลสารสนเทศด้วย

“ทรัพย์สิน”
หมายถึง ข้อมูลโปรแกรม เอกสาร อุปกรณ์ เครื่องมือ เครื่องใช้ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ และระบบเทคโนโลยีสารสนเทศที่บริษัท เป็นเจ้าของ หรือ เป็นการจัดทำและพัฒนาขึ้นมา

“ผู้ใช้งาน”
หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถใช้งานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของบริษัทโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

“ผู้ดูแลระบบ”
หมายถึง พนักงานที่กลุ่มบริษัท ดำเนินการแต่งตั้งให้ทำหน้าที่ดูแล บำรุงรักษา และแก้ไขอุปกรณ์คอมพิวเตอร์ รวมทั้งทำหน้าที่ในการกำหนดสิทธิในการใช้งานระบบคอมพิวเตอร์ รวมทั้งระบบเครือข่ายให้กับผู้ใช้งาน

“หน่วยงานภายนอก”
หมายถึง บริษัทหรือหน่วยงานที่บริษัทอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“เจ้าของข้อมูล”
หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิของผู้ใช้งาน”
หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

“รหัสผ่าน”
หมายถึง กลุ่มข้อความที่ประกอบตัวอักษร ตัวเลข หรืออักขระพิเศษที่กำหนดให้ผู้ใช้งานระบบสารสนเทศระบุตัวตน และสิทธิในการเข้าใช้งานระบบสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูล

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”
หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

“ระบบเครือข่าย”
หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัทได้

“อินเทอร์เน็ต” หมายถึง เครือข่ายภายนอกที่เชื่อมต่อกันทั่วโลก

“อินทราเน็ต” หมายถึง เครือข่ายภายในบริษัท

“จดหมายอิเล็กทรอนิกส์”
หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดนผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่ง โดยจะเป็นได้ทั้ง ตัวอักษร ภายถ่าย ภาพกราฟ ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนได้

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์”
หมายถึง สถานการณ์ด้านความมั่งคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบของบริษัทถูกบุกรุกหรือโจมตี และถูกคุกคาม

“ผู้บังคับบัญชา”
หมายถึง พนักงานที่ได้รับการแต่งตั้งจากกลุ่มบริษัท ให้ดำรงตำแหน่งหัวหน้าส่วนใดส่วนหนึ่งทั้งในด้านการปฏิบัติ การบังคับบัญชาพนักงาน การควบคุม และการดำเนินงานให้เป็นไปตามระเบียบข้อบังคับของกลุ่มบริษัท และระเบียบปฏิบัติซึ่งผู้บังคับบัญชาชั้นเหนือตนขึ้นไป

หมวดที่ 1

การสำรองข้อมูลและการกู้คืน (Backup and Recovery)

วัตถุประสงค์

เพื่อให้การดำเนินงานการสำรองข้อมูลและการกู้คืนระบบเป็นไปอย่างเหมาะสมมีความมั่นคงปลอดภัย โดยสามารถรักษาความถูกต้องและพร้อมใช้งานของข้อมูลสารสนเทศ พร้อมทั้งมีการป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข การลบหรือทำลายสื่อที่ใช้เก็บข้อมูลโดยไม่ได้รับอนุญาต

การสำรองข้อมูล

1.1 กำหนดให้มีการสำรองข้อมูลสำคัญทางธุรกิจ ลงในสื่อบันทึกข้อมูลสำรอง โดยสามารถกู้ข้อมูลกลับคืนได้ย้อนหลังอย่างน้อย 7 วัน รวมถึงโปรแกรมระบบปฏิบัติการ โปรแกรมระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้งานให้ครบถ้วน เพื่อให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

1.2 กำหนดให้มีขั้นตอน หรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานและต้องทำเอกสารขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการเป็นลายลักษณ์อักษรทุกครั้งที่มีการแก้ไขเพิ่มเติมกระบวนการสำรองข้อมูล (Job Backup)

1.3 กำหนดให้มีการบันทึกการปฏิบัติงานทุกวันเกี่ยวกับการสำรองข้อมูลและการกู้คืนข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน

การกู้คืนข้อมูล

1.4 กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้งเพื่อให้มั่นใจว่าข้อมูล รวมทั้งโปรแกรมต่าง ๆ ที่สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้

1.5 กำหนดให้มีขั้นตอน หรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อที่บันทึกมาใช้งาน โดยให้มีการทดสอบข้อมูลก่อนการใช้งานจริงเพื่อป้องกันข้อมูลผิดพลาดทั้งนี้ต้องจัดทำเอกสารประกอบการทดสอบข้อมูลโดยมีการลงนามตามรายชื่อผู้เกี่ยวข้องกับข้อมูลหรือผู้ใช้ข้อมูล ร่วมปฏิบัติการทดสอบทุกครั้ง

1.6 เมื่อมีความจำเป็นต้องกู้คืนข้อมูล จากระบบสำรองไม่ว่าจะกรณีใดต้องทำเอกสารขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการ เป็นลายลักษณ์อักษรทุกครั้ง

1.7 หากมีความเสียหายเกิดขึ้นกับระบบฐานข้อมูล หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งาน(ผู้เป็นเจ้าของข้อมูล)ทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้น

1.8 กรณีที่การกู้ข้อมูลมีผลกระทบต่อข้อมูลในส่วนงานอื่น ให้แจ้งต่อหน่วยงานที่ได้รับผลกระทบทราบก่อนดำเนินการกู้คืนระบบ

การเก็บรักษาและการจัดการสื่อบันทึก

1.9 สำหรับระบบงานที่มีความสำคัญสูง ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ทำงานปัจจุบันไม่สามารถเคลื่อนย้ายได้

1.10 ควรมีขั้นตอนการจัดการสื่อบันทึกข้อมูลสารสนเทศสำคัญที่สามารถเคลื่อนย้ายได้ (External Hard disk) ไว้ในที่ที่ปลอดภัย เช่น ตู้นิรภัยเป็นต้น

1.11 ควรติดป้ายชื่อที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

1.12 ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่าง ๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน Recycle Bin

หมวดที่ 2

การดำเนินงานระบบสารสนเทศและเครือข่าย (Information and Network Security)

วัตถุประสงค์

เพื่อให้การดำเนินงานเครือข่าย เป็นไปอย่างเหมาะสมมีความมั่นคงปลอดภัย สามารถรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยโปรแกรมไม่พึงประสงค์ สามารถป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย และมีการตรวจจับการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต โดยให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างถูกต้อง

การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย

2.1 มีการกำหนดชั้นความลับข้อมูล รวมถึงการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ

2.2 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL หรือ VPN

การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

2.3 มีขั้นตอนตรวจสอบหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์ และเมื่อพบว่าการใช้งานมีลักษณะผิดปกติต้องรีบดำเนินการแก้ไข

2.4 ต้องเปิดบริการ (Service) เท่าที่จำเป็นหากบริการที่ใช้ความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

2.5 ต้องดำเนินการติดตั้ง Patch ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ ระบบฐานข้อมูลโปรแกรมประยุกต์ต่างๆและระบบเว็บที่พัฒนาขึ้น เป็นต้น เพื่ออุดช่องโหว่ต่าง ๆ อย่างสม่ำเสมอ

2.6 ควรตรวจสอบซอฟต์แวร์ที่ใช้เกี่ยวกับความปลอดภัย และประสิทธิภาพการใช้งานทั่วไปก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

2.7 ควรมีแนวทางปฏิบัติในการใช้ซอฟต์แวร์ตรวจสอบระบบความปลอดภัย เช่น Firewall, Personal Firewall เป็นต้น

2.8 ต้องกำหนดให้มีการระบุผู้รับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมอย่างชัดเจนพร้อมทั้งทำเอกสารขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการ เป็นลายลักษณ์อักษรทุกครั้ง

การบริหารจัดการ และการตรวจสอบระบบเครือข่าย

2.9 ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น เครือข่ายภายใน (Internal Zone) เครือข่ายภายนอก (External Zone) และเครือข่ายพิเศษ (Demilitarized: DMZ) เป็นต้น

2.10 ต้องมีระบบป้องกันการบุกรุก เช่น Firewall หรือ IDS, IPS ระหว่างเครือข่ายภายใน และภายนอก เป็นต้น

2.11 ต้องมีระบบตรวจสอบการบุกรุก และการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยต้องมีการตรวจสอบอย่างสม่ำเสมอ

2.12 ต้องตรวจสอบเกี่ยวกับความปลอดภัยอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบภัยคุกคามทางระบบคอมพิวเตอร์ ตรวจสอบการกำหนดค่าพารามิเตอร์ต่างๆ เกี่ยวกับความปลอดภัย และการตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อ (Disable Port) ที่ไม่จำเป็น

2.13 กรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ Remote Access หรือการเชื่อมต่อเครือข่ายภายนอก โดยใช้ Client VPN ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ในการควบคุมอย่างเข้มงวด และต้องมีการตรวจสอบตัวตนจริงของผู้ใช้งาน

2.14 ต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลงค่าพารามิเตอร์ต่างๆ ของระบบเครือข่าย และการเชื่อมต่อระบบเครือข่ายอย่างชัดเจน พร้อมทั้งทำเอกสารขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการ เป็นลายลักษณ์อักษรทุกครั้ง

2.15 กำหนดการใช้เครื่องมือต่างๆ (Tools) เพื่อตรวจสอบเช็คระบบเครือข่าย ควรได้รับอนุมัติจากผู้มีอำนาจดำเนินการ

การติดตั้ง ปรับเปลี่ยนซอฟต์แวร์ และการวางแผนประสิทธิภาพระบบ

2.16 การติดตั้งซอฟต์แวร์ต่าง ๆ ต้องทำอย่างถูกลิขสิทธิ์ บริษัทไม่อนุญาตให้พนักงานติดตั้งซอฟต์แวร์ใดๆ ที่บริษัทยังไม่ได้จัดซื้อมาให้ถูกต้องตามกฎหมาย หรือกระทำโดยภาระการ

2.17 ก่อนการเปลี่ยนแปลงระบบ และอุปกรณ์คอมพิวเตอร์ควรมีการประเมินผลกระทบที่เกี่ยวข้อง ภายหลังจากการเปลี่ยนแปลงระบบ ให้มีการตรวจสอบการทำงานระบบ และบันทึกการเปลี่ยนแปลงให้เป็นปัจจุบันเสมอพร้อมทั้งทำเอกสารขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการ เป็นลายลักษณ์อักษรทุกครั้ง

2.18 ทำการประเมินการใช้งานระบบคอมพิวเตอร์ไว้ล่วงหน้า เพื่อรองรับการใช้งานในอนาคต

การป้องกันภัยคุกคามทางระบบคอมพิวเตอร์ และโค้ดมุ่งร้าย (Malicious Code)

2.19 เครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่องต้องติดตั้งซอฟต์แวร์ป้องกันภัยคุกคามทางระบบคอมพิวเตอร์ที่มีประสิทธิภาพ และปรับปรุงให้เป็นปัจจุบัน

2.20 ต้องกำหนดให้มีการ Scanning Virus ที่เครื่องของผู้ใช้งาน แบบอัตโนมัติในเวลา 12.00 น. ของทุกวันทำการ และต้องกำหนดให้มีการ Update Virus Signature Database และ Update Patch Windows O/S อยู่เสมอ

2.21 ฝ่ายคอมพิวเตอร์ต้องจัดทำคู่มือในการป้องกันภัยคุกคามทางระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมถึงแนะนำวิธีการ พร้อมทั้งให้ความรู้แก่ผู้ใช้งานเกี่ยวกับภัยคุกคามทางระบบคอมพิวเตอร์ชนิดใหม่

2.22 กำหนดให้มีมาตราการ การป้องกันควบคุมการระงับการใช้งานซอฟต์แวร์ที่ไม่พึงประสงค์ ทันทีพร้อมทั้งแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีภัยคุกคามทางระบบคอมพิวเตอร์

การบันทึกเพื่อตรวจสอบ (Audit logs)

2.23 ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่าย และเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น การบักทึกความพยายามในการเข้าใช้ระบบบันทึกใช้คำสั่ง Command line และการเก็บบันทึกล็อกไฟล์

2.24 การบันทึกการเข้าใช้งาน (ข้อมูลจราจรคอมพิวเตอร์) ของผู้ใช้และผู้ดูแลระบบ อย่างน้อย 180 วัน

2.25 ต้องมีระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

การใช้งานอินเตอร์เน็ต

2.26 การใช้อินเตอร์เน็ต บริษัทจะพิจารณาอนุญาตให้ใช้งานตามความจำเป็น ทั้งนี้ให้ผู้ใช้งาน ทำเอกสารขออนุมัติผู้บังคับบัญชาตามสายงานที่ตนปฏิบัติงาน และเมื่อมีการอนุมัติแล้ว จึงแจ้งให้ผู้ดูแลระบบดำเนินการเปิดสิทธิให้ใช้งานได้ พร้อมทั้งปฏิบัติตามกฎหมายอย่างเคร่งครัด

2.27 ให้มีการพิจารณาเนื้อหาและบริการที่เหมาะสมกับความจำเป็นในการใช้งาน ทั้งนี้ให้อยู่ในดุลยพินิจของผู้บังคับบัญชาตามสายงานที่พนักงานปฏิบัติงาน

2.28 ห้ามมิให้พนักงานอัลโหลดหรือโพสต์รูปภาพข้อมูลที่มีภัยคุกคามทางระบบคอมพิวเตอร์ ข้อมูลที่มีชุดคำสั่งไม่พึงประสงค์หรือข้อมูลใดๆ อันไม่เกี่ยวข้องกับบริษัทฯ บนเว็บไซต์ของบริษัทและ/หรือเว็บไซต์ต่างๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.29 ห้ามมิให้พนักงานดาวน์โหลดรูปภาพข้อมูลที่มีภัยคุกคามทางระบบคอมพิวเตอร์ ข้อมูลที่มีชุดคำสั่งไม่พึงประสงค์หรือข้อมูลใดๆที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผ่านระบบเครือข่ายของบริษัท

การติดต่อสื่อสารทางอิเล็กทรอนิกส์

2.30 กำหนดขนาดข้อมูลสารสนเทศที่รองรับในจดหมายอิเล็กทรอนิกส์ได้ครั้งละไม่เกิน 30 MB เพื่อรองรับการใช้งานได้อย่างมีประสิทธิภาพ

2.31 ผู้ใช้งานไม่ควรส่งข้อความ และไฟล์แนบขนาดใหญ่เกิน 10 MB

2.32 ในการติดต่อสื่อสารทางอิเล็คทรอนิกส์ ไม่ว่าจะเป็นจดหมายอิเล็คทรอนิกส์ การสนทนา หรือการติดต่อสื่อสารใดๆ ให้ถือเสมือนหนึ่งการส่งจดหมายแบบเป็นทางการโดยจะต้องปฏิบัติตามกฎการรับ-ส่งหนังสือหรือจดหมายของบริษัท

2.33 พนักงานพึงใช้ข้อความสุภาพ หรือใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น รวมทั้งปฏิบัติให้ถูกต้องตามธรรมเนียมปฏิบัติของการส่งจดหมายอิเล็คทรอนิกส์ การสนทนา หรือการสื่อสารทางอิเล็คทรอนิกส์อื่นๆ ในระบบเครือข่าย

2.34 ห้ามมิให้พนักงานส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อ บริษัท หรือบุคคลอื่นๆ หรือส่งรูปภาพ หรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร หรือส่งข้อความที่ไม่เหมาะสม เช่นคำหยาบคาย คำด่าทอ หรือข้อความก้าวร้าวทั้งนี้การส่งข้อมูลใดๆ ให้พนักงานปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยบริษัทสงวนสิทธิในการตรวจสอบข้อความในจดหมายอิเล็กทรอนิกส์ทั้งหมด

2.35 ห้ามมิให้พนักงานกระทำการใดๆ ที่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยผ่านระบบเครือข่ายคอมพิวเตอร์ของ บริษัท

การใช้งานสังคมออนไลน์

2.36 ไม่อนุญาตให้เผยแพร่ข้อมูลที่สำคัญของบริษัท ข้อมูลที่เป็นความลับ ข้อมูลทรัพย์สินของบริษัท รวมถึงข้อตกลง สัญญา หรือสัญญากับคู่ค้าในระหว่างการดำเนินการ

2.37 ควรหลีกเลี่ยงบทสนทนาที่อ้างถึงบริษัท โดยไม่อนุญาตให้อ้างถึงบริษัทในลักษณะที่ส่งผลกระทบต่อภาพลักษณ์ของบริษัทในทางที่ไม่ดี

2.38 ผู้ใช้ควรระมัดระวัง ไม่ตกเป็นเหยื่อของโปรแกรมที่ไม่พึงประสงค์

2.39 กรณีที่การใช้สังคมออนไลน์ต่างๆ (เช่น Facebook, Twitter,Google+ , Line ฯลฯ)ส่งผลกระทบต่อการปฏิบัติงานที่ได้รับมอบหมายผู้บังคับบัญชาสามารถกำหนดช่วงเวลาเพื่อระงับการใช้งานได้

2.40 บริษัทสงวนสิทธิในการตรวจสอบข้อความในสื่อสังคมออนไลน์ต่างๆ ที่ผ่านระบบเครือข่ายของบริษัท

หมวดที่ 3

การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกและจากชุดคำสั่งที่ไม่พึงประสงค์ที่อาจสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศ (ระดับความสำคัญ: สูง)

การควบคุมสิทธิแก่ผู้ใช้

3.1 ต้องกำหนดสิทธิการใช้ข้อมูล และระบบคอมพิวเตอร์ เช่น การใช้โปรแกรมคอมพิวเตอร์(Application System) สิทธิการใช้งานอินเตอร์เน็ต โดยผู้ใช้ต้องได้รับสิทธิเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร

3.2 กรณีที่มีความจำเป็นต้องใช้ผู้ใช้มีสิทธิพิเศษ ต้องมีการควบคุมการเข้าใช้อย่างรัดกุม

3.3 ในกรณีที่มีความจำเป็นต้องให้ผู้ใช้งานเป็นเจ้าของข้อมูล และมีการให้สิทธิแก่ผู้อื่นเข้าใช้งาน ต้องมีการระบุเฉพาะราย หรือเฉพาะกลุ่มเท่านั้น และมีการกำหนดอายุการใช้งาน และระงับทันทีที่พ้นระยะการใช้งาน

3.4 กำหนดให้มีการตรวจทานสิทธิการใช้งานระบบคอมพิวเตอร์ และทะเบียนรายชื่อผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อความปลอดภัย

การควบคุมการใช้งานบัญชีรายชื่อที่มีสิทธิสูงสุดของระบบ (User: Administrator) และรหัสผ่าน

3.5 กำหนดให้ User : Administrator เป็น User Account ที่มีสิทธิสูงสุดของระบบ และกำหนดให้ User : SA เป็น User Account ที่มีสิทธิสูงสุดของระบบฐานข้อมูล ซึ่งใช้สำหรับการติดตั้ง แก้ไข ปรับปรุงและเปลี่ยนแปลงระบบปฏิบัติการ และระบบฐานข้อมูลตามลำดับ ทั้งนี้ให้ดำเนินการจัดเก็บรักษารหัสผ่านไว้ในที่ที่ปลอดภัย โดยทำเป็นเอกสารใส่ซองปิดผนึก กำหนดให้รองกรรมการผู้จัดการสายงานระบบปฏิบัติการ เป็นผู้เก็บรักษา และมีอำนาจลงนามกำกับซองเอกสารรหัสผ่านร่วมกับกรรมการผู้จัดการหรือรองกรรมการผู้จัดการสายงานอีกท่าน

3.6 หากมีความจำเป็นต้องใช้ User : Administrator และ User : SA ในการแก้ไขเปลี่ยนแปลงระบบใดๆ ให้ทำเอกสารขออนุมัติดำเนินการเป็นครั้งๆ ไป โดยให้รองกรรมการผู้จัดการสายงานระบบปฏิบัติการเป็นผู้ใส่รหัสผ่านทุกครั้ง

3.7 ให้มีการตรวจสอบระบบเพื่อเปลี่ยนแปลงรหัสผ่าน User : Administrator และ User : SA อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงทุกครั้ง ต้องจัดเก็บรักษารหัสผ่าน โดยทำเป็นเอกสารใส่ซองปิดผนึกไว้ดังเดิม

การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน

3.8 บริษัท จะจัดให้มีชื่อผู้ใช้ (USER ID) และรหัสผ่าน (Password) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบเครือข่ายคอมพิวเตอร์และการเชื่อมต่อกับอินเทอร์เน็ตเป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่านดังนี้

3.8.1 มีความยาวของตัวอักษรไม่น้อยกว่า 8 ตัวอักษร

3.8.2 ตัวอักษรสามารถใช้ร่วมกันได้ทั้งตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และสามารถใช้ร่วมกับอักขระพิเศษ และตัวเลข ผสมกัน

3.8.3 ไม่ใช้ข้อมูลส่วนตัวของผู้ใช้งานมาตั้งเป็นรหัสผ่าน เช่น ชื่อ นามสกุล วันเดือนปีเกิด รหัสพนักงาน ที่อยู่ เบอร์โทรศัพท์ ฯลฯ

3.8.4 กำหนดให้มีระยะเวลาที่ต้องเปลี่ยนรหัส ภายในเวลา 90 วัน และรหัสผ่านที่ตั้งจะไม่สามารถตั้งซ้ำกันได้ใน 24 ครั้ง ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม และให้มีการตรวจสอบการพิมพ์รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง หากเกินให้ระบบล็อค User Account ทันทีและจะปลดล็อคอัตโนมัติภายใน 30 นาทีทั้งนี้ผู้ใช้งานสามารถแจ้งให้ผู้ดูแลระบบเป็นผู้ปลดล็อดเพื่อใช้งานได้

3.8.5 ต้องมีระบบตรวจสอบตัวตนจริง และสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication)ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ โดยผู้ใช้ทุกคนต้องมี User Account ของตนเอง

3.9 กำหนดให้มีการควบคุมและบริหารจัดการสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน ตามที่ผู้ใช้งานได้ดำเนินการขออนุมัติดำเนินการจากผู้บริหารที่มีอำนาจอนุมัติดำเนินการ เป็นลายลักษณ์อักษรแล้ว

3.10 รหัสผ่านของพนักงานถือเป็นทรัพย์สินของบริษัท ไม่อนุญาตให้มีการแจ้งรหัสผ่านที่เป็นข้อมูลส่วนตัวให้กับบุคคลอื่น และพนักงานทุกคนมีหน้าที่ในการป้องกันรหัสผ่านของบริษัทอย่างเคร่งครัด

3.11 บริษัท ไม่อนุญาตให้ใช้ชื่อและรหัสผ่านร่วมกัน ทั้งนี้พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่พึงอนุญาตให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง และเพื่อเป็นการป้องกันหากมีผู้อื่นล่วงรู้และนำรหัสผ่านของพนักงานไปใช้ในทางที่ผิดและเกิดความเสียหายต่อบริษัท พนักงานจะต้องเก็บรหัสผ่านไว้เป็นความลับ และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่

3.12 พนักงานที่ได้รับมอบหมายให้เข้าใช้ระบบงานต่างๆที่ บริษัท กำหนดให้ใช้ พนักงานจะต้องปฏิบัติตามกฎการใช้ระบบและเก็บรักษาชื่อและรหัสผ่านไว้ ห้ามมิให้เปิดเผยกับผู้อื่น ยกเว้นได้รับอนุมัติจากผู้บังคับบัญชาโดยตรงเป็นลายลักษณ์อักษร

3.13 หากจะต้องมีการเลิกใช้ชื่อและรหัสผ่าน ให้แจ้งกับผู้บังคับบัญชาโดยตรงเพื่อทำเรื่องขอเลิกใช้โดยจะต้องกระทำทันทีที่จะเลิกใช้งาน

3.14 ในกรณีที่พนักงานลาออก ,เกษียณอายุ หรือมีเหตุที่ต้องออกจากงาน ผู้บังคับบัญชามีหน้าที่ต้องแจ้งขอยกเลิกการใช้งานชื่อและรหัสผ่านของพนักงานผู้นั้นโดยทันที

การควบคุมการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ และระบบสารสนเทศ

3.15 ต้องมีการพิสูจน์ตัวตนบนเครือข่าย โดยกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมโยงนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

3.16 การเข้าถึงระบบปฏิบัติการ ต้องมีการระบุและพิสูจน์ตัวตนของผู้ใช้งานที่ไม่ซ้ำซ้อนกัน

3.17 การเข้าถึงสารสนเทศระบบงาน ต้องมีการจำกัดการเข้าถึงข้อมูลและฟังก์ชันของระบบตามขอบเขตสิทธิที่ได้รับอนุญาต

หมวดที่ 4

การสร้างความปลอดภัยด้านกายภาพ (Physical Security)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และเพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินของบริษัท และการทำให้กิจกรรมการดำเนินงานต่างๆ ของบริษัทเกิดการติดขัดหรือหยุดชะงัก (ระดับความสำคัญ: ปานกลาง)

การเข้าออกศูนย์คอมพิวเตอร์

4.1 ต้องเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย ในพื้นที่ที่ปลอดภัย

4.2 มีระบบตรวจสอบบุคคลเข้า/ออก ห้องควบคุม (Server Room) และมีการตรวจสอบอย่างรัดกุม โดยให้ถือปฏิบัติตามระเบียบการเข้า/ออก ห้องควบคุม (Server Room)

การป้องกันความเสียหาย

4.3 ห้องคอมพิวเตอร์ต้องมีอุปกรณ์ป้องกันไฟไหม้ห้องคอมพิวเตอร์

4.4 ต้องมีระบบสำรองไฟฟ้าห้องคอมพิวเตอร์

4.5 ต้องมีระบบปรับอากาศและระบบตรวจสอบความชื้น

หมวดที่ 5

การบริหารความต่อเนื่องในการดำเนินงานของบริษัท

วัตถุประสงค์

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ มุ่งเน้นการป้องกันกระบวนการธุรกิจที่สำคัญจากความล้มเหลวของระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม (ระดับความสำคัญ: ปานกลาง)

การบริหารความเสี่ยงสารสนเทศ

5.1 ระบุความเสี่ยง และเหตุการณ์ความเสี่ยงที่สำคัญหรือเหตุการณ์รุนแรงลักษณะฉับพลัน สามารถนำไปสู่การหยุดชะงัก ความเสียหายของระบบงานสารสนเทศ เพื่อทำการประเมินความเสี่ยง โดยการระบุความเสี่ยงควรกล่าวถึงเหตุการณ์ฉุกเฉินดังต่อไปนี้

- ตามเหตุการณ์: กรณีอาคารถูกปิดล้อมไม่สามารถเข้ามาในตัวอาคารได้
- ตามความรุนแรง/พื้นที่: ไหม้ห้องควบคุม (Server Room), ไหม้หน่วยงานสารสนเทศ, ไฟไหม้อาคาร, น้ำท่วมบริเวณพื้นที่อาคาร, กรณีระบบล่มทั้งบริษัท

5.2 กำหนดวิธีการประเมินความเสี่ยงและความรุนแรงของผลกระทบ

5.3 กำหนดมาตรการจัดการความเสี่ยง จัดทำหรือทบทวนแผนแก้ไขปัญหาจากความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Continuity Plan)

หมวดที่ 6

การจัดหา พัฒนา และปรับปรุงระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐาน เพื่อป้องกันความผิดพลาดในการประมวลผลระบบสารสนเทศ หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต เพื่อสร้างความปลอดภัยให้กับไฟล์ต่างๆของระบบ (ระดับความสำคัญ: ปานกลาง)

การพัฒนาระบบงาน

6.1 ควรแบ่งแยกคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้เกี่ยวข้องในแต่ละส่วนเท่านั้น

6.2 ผู้ที่ร้องขอรวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ

6.3 ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

6.4 ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ให้เป็นปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไข เปลี่ยนแปลงที่ผ่านมา

6.5 ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลงให้ทันสมัยอยู่เสมอ

การทดสอบระบบ

6.6 ผู้ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นๆที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพและประมวลผลได้ครบถ้วนถูกต้อง

6.7 ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน

การสื่อสารการเปลี่ยนแปลง

6.8 ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

หมวดที่ 7

โครงสร้างความปลอดภัยระบบสารสนเทศภายนอกและภายในบริษัท

วัตถุประสงค์

เพื่อบริการจัดการความปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลที่ถูกเข้าถึงจากหน่วยงานภายนอก ภายในบริษัทและเพื่อให้พนักงานเข้าใจถึงบทบาทความรับผิดชอบ ลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติงาน (ระดับความสำคัญ: พื้นฐาน)

การคัดเลือกผู้ให้บริการ

7.1 ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุม และเป็นที่น่าเชื่อถือ

7.2 ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) อย่างชัดเจน

7.3 ควรมีสัญญาที่ระบุเกี่ยวกับระยะเวลาดำเนินการ หรือแก้ไขปัญหา และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

การควบคุมผู้ให้บริการ

7.4 ในกรณีที่ใช้บริการด้านการพัฒนาระบบงานต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Development Environment) เท่านั้น หากต้องให้เข้าใช้ระบบงานจริง (Production Environment) ต้องมีการควบคุม และการตรวจสอบผู้ให้บริการอย่างเข้มงวด

7.5 ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

7.6 ควรกำหนดให้ผู้ให้บริการรายงานปัญหาต่างๆ และแนวทางการแก้ไข ในการปฏิบัติงาน

7.7 ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

การรับมือเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์

7.8 กำหนดเหตุการณ์ที่ละเมิดความปลอดภัยด้านคอมพิวเตอร์

7.9 จัดทำเอกสารเผยแพร่ต่อเหตุการณ์ที่ละเมิดความปลอดภัยด้านคอมพิวเตอร์

7.10 กำหนดขั้นตอนในการรับมือเหตุการณ์ต่างๆ โดยมีการตรวจสอบ และวิเคราะห์ผู้เข้ามาจู่โจมระบบ

7.11 กำหนดวิธีลบ และกู้คืนข้อมูล

ความปลอดภัยภายในบริษัท

7.12 ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับบริษัทว่าจะไม่เปิดเผยความลับของบริษัท (โดยการลงนามนี้เป็นส่วนหนึ่งในการว่าจ้างพนักงาน)

7.13 ควรกำหนดให้มีการทบทวนการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความปลอดภัยสารสนเทศโดยผู้ตรวจสอบอิสระ

ด้านบุคลากรสารสนเทศ

7.14 ควรกำหนดหน้าที่ความรับผิดชอบด้านความปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร สำหรับพนักงาน

7.15 ต้องจัดให้มีกระบวนการลงโทษทางวินัยเพื่อลงโทษหรือละเมิดระเบียบปฏิบัติ

7.16 ต้องทำการถอดถอนสิทธิการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศเมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้าง

หมวดที่ 8

การจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อป้องกันทรัพย์สินของบริษัทจากความเสียหายที่อาจจะเกิดขึ้นได้ และเพื่อกำหนดระดับของการป้องกันสารสนเทศของบริษัทอย่างเหมาะสม (ระดับความสำคัญ: พื้นฐาน)

การจัดการทรัพย์สินสารสนเทศ

8.1 ต้องจัดทำบัญชีทรัพย์สินสารสนเทศ เช่น ข้อมูลสารสนเทศ, ระบบงานสารสนเทศ, อุปกรณ์สารสนเทศ และอื่นๆ โดยมีการกำหนดระดับความสำคัญของทรัพย์สิน การเป็นความลับของทรัพย์สิน เพื่อใช้ประกอบการพิจารณาในการบริหารจัดการ

8.2 กำหนดผู้รับผิดชอบทรัพย์สินสารสนเทศ

8.3 กำหนดระดับการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

หมวดที่ 9

การจัดการสถานการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนด้านความปลอดภัยของระบบสารสนเทศได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม (ระดับความสำคัญ: พื้นฐาน)

การจัดการเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับระบบสารสนเทศ

9.1 ควรจัดทำบันทึกและมีการรายงานจุดอ่อนที่เกี่ยวกับความปลอดภัยระบบสารสนเทศที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

9.2 ควรกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ได้อย่างรวดเร็วอย่างเป็นระบบระเบียบ

9.3 ควรเรียนรู้จากเหตุการณ์ละเมิดความปลอดภัย โดยพิจารณาถึงสาเหตุ ปริมาณที่เกิด และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อเตรียมการรับมือล่วงหน้า

บทลงโทษ

พนักงานมีหน้าที่ต้องปฏิบัติอย่างเคร่งครัด ถ้าพนักงานผู้ใดปฏิบัติใด ๆ อันถือได้ว่าเป็นการฝ่าฝืนวินัยดังกล่าวจะต้องถูกพิจารณาลงโทษมางวินัยโดยกลุ่มบริษัท กำหนดบทลงโทษวินัยไว้ 4 ประการดังนี้

1. การตักเตือนด้วยวาจา
2. การตักเตือนเป็นหนังสือ
3. การพักงานโดยไม่ได้รับค่าจ้าง ไม่เกิน 7 วัน
4. การเลิกจ้างโดยไม่จ่ายค่าชดเชย และ/หรือรับผิดตามกฎหมาย โดยส่งดำเนินคดี

หลักเกณฑ์การพิจารณาลงโทษทางวินัย

1. การพิจารณาลงโทษทางวินัย โดยการตักเตือนด้วยวาจา เมื่อการกระทำผิดทางวินัยนั้นปรากฏผลดังนี้
   - 1.1 การผิดวินัยนั้นยังไม่ก่อให้เกิดผลเสียต่อบริษัท
   - 1.2 ผู้กระทำผิดวินัยไม่เคยกระทำผิดในเรื่องเดียวกันนี้มาก่อน
   - 1.3 เมื่อพนักงานได้สำนึกว่าตนได้กระทำผิดวินัย และรับรองว่าจะไม่กระทำผิดอีก
   - 1.4 ถ้าฝ่าฝืนวินัยใดๆ มีพฤติกรรมผลลัพท์แตกต่างจากหลักเกณฑ์ 3 ข้อนี้ไม่ว่าจะเป็นข้อใดข้อหนึ่ง จะพิจารณาลงโทษตามบทลงโทษอื่นๆ ต่อไป การลงโทษโดยการตักเตือนด้วยวาจานั้น เมื่อผู้บังคับบัญชาได้ทำการลงโทษไปแล้ว ให้ทำบันทึกรายละเอียดพฤติกรรม เวลา สถานที่ บุคคลที่เกี่ยวข้อง และรายละเอียดอื่นๆ อันเกี่ยวข้องกับการกระทำความผิดของพนักงานแล้วส่งไปยังฝ่ายบุคคลโดยเร็วที่สุด
2. การพิจารณาโทษทางวินัย โดยการตักเตือนเป็นหนังสือ การตัดค่าจ้าง หรือสั่งพักงาน มีหลักเกณฑ์ในการพิจารณาโทษดังนี้
   - 2.1 เมื่อเจตนากระทำความผิดทางวินัยหรือทำผิดวินัยซ้ำในเรื่องเดิม
   - 2.2 ผู้พิจารณาลงโทษเห็นว่า การลงโทษโดยการตักเตือนด้วยวาจา จะไม่ประสบผลให้พิจารณาลงโทษ ดังนี้
     - 2.2.1 ตักเตือนเป็นหนังสือ
     - 2.2.2 สั่งพักงาน
3. การพิจารณาลงโทษทางวินัย โดยการเลิกจ้างโดยไม่จ่ายค่าชดเชยจะลงโทษเมื่อพนักงานกระทำการในกรณีหนึ่งกรณีใด ดังต่อไปนี้
   - 3.1 ทุจริตต่อหน้าที่
   - 3.2 กระทำผิดอาญาโดยเจตนาต่อกลุ่มบริษัท

3.3 จงใจทำให้กลุ่มบริษัทได้รับความเสียหาย

3.4 ฝ่าฝืนข้อบังคับเกี่ยวกับการทำงาน หรือระเบียบ หรือคำสั่งของกลุ่มบริษัท อันชอบด้วยกฎหมายและได้ตักเตือนเป็นหนังสือแล้ว เว้นแต่กรณีร้ายแรง กลุ่มบริษัท ไม่จำเป็นต้องตักเตือนก่อน หนังสือมีผลบังคับไม่เกินหนึ่งปีนับตั้งแต่วันที่ลูกจ้างได้กระทำผิด

3.5 ละทิ้งหน้าที่เป็นเวลา 3 วันทำงานติดต่อกัน ไม่ว่าจะเป็นวันหยุดคั่นหรือไม่ก็ตาม โดยไม่มีเหตุผลอันสมควร

3.6 ประมาทเลินเล่อเป็นเหตุให้กลุ่มบริษัท ได้รับความเสียหายอย่าร้ายแรง

3.7 ได้รับโทษจำคุกตามคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

4. การพิจารณาลงโทษและบทลงโทษสำหรับการกระทำผิดทางวินัยนั้นข้อบังคับของกลุ่มบริษัทตามที่ได้กล่าวมาแล้วนั้นยังไม่ละเอียดและครอบคลุมถึงสถานการณ์ได้ ดังนั้นการพิจารณาลงโทษหรือการกำหนดบทลงโทษให้อยู่ให้อยู่ในดุลยพินิจของกลุ่มบริษัท ทั้งนี้คำนึงถึงการสร้างสรรค์เพื่อให้เกิดความเป็นธรรม และเสมอภาคแก่พนักงานทุกคน

5. รายละเอียดเพิ่มเติมเกี่ยวกับการลงโทษทางวินัย

5.1 อายุของคำเตือนพนักงานที่กระทำความผิดวินัยและถูกเตือนด้วยวาจา หรือหนังสือให้มีผลบังคับได้ไม่เกินหนึ่งปี นับแต่วันที่ลูกจ้างกระทำผิด

5.2 เมื่อการกระทำผิดในคราวเดียว เป็นความผิดต่อข้อบังคับหลายข้อให้ใช้ข้อบังคับที่มีโทษหนักที่สุดลงโทษแก่ผู้กระทำความผิด

5.3 การกระทำผิดหลายกระทงในเวลาไล่เลี่ยกัน เมื่อพนักงานกระทำความผิดหลายอย่างในเวลาไล่เลี่ยกันถึงแม้ว่ากลุ่มบริษัท อาจได้ดำเนินการลงโทษทางวินัยอย่างทันทีแล้วก็ตามก็ยังไม่ทันต่อเหตุการณ์ เพราะได้มีการกระทำความผิดอื่น ๆ อีกในเวลาไล่เลี่ยกัน ในกรณีนี้กลุ่มบริษัทอาจจะพิจารณาลงโทษทางวินัยหนักกว่าโทษสำหรับความผิดที่ถือว่าหนักที่สุดในบรรดาความผิดที่พนักงานได้กระทำไปนั้น

5.4 ในระหว่างพิจารณาโทษทางวินัย กลุ่มบริษัท มีสิทธิ์สั่งพักงานพนักงานเพื่อการสอบสวนได้ไม่เกิน 7 วัน โดยไม่จ่ายค่าจ้างให้ห้าสิบเปอร์เซ็นต์ และเมื่อมีการสอบสวนเสร็จสิ้นแล้ว หากปรากฏว่าพนักงานไม่มีความผิด กลุ่มบริษทจะจ่ายค่าจ้างให้แก่พนักงานเท่ากับค่าจ้างในวันทำงานนับตั้งแต่วันที่ลูกจ้างถูกสั่งพักงาน

6. ผู้มีอำนาจพิจารณาและดำเนินการลงโทษทางวินัย

6.1 การลงโทษ ผู้บังคับบัญชาโดยตรงของพนักงานผู้กระทำความผิดร่วมกับผู้บังคับบัญชาระดับเหนือขึ้นไปอีกชั้นหนึ่งเป็นผู้พิจารณาและดำเนินการลงโทษ

เอกสารประกอบ 1
หน้าที่และความความรับผิดชอบเจ้าหน้าที่สารสนเทศ

เพื่อความเป็นระเบียบเรียบร้อยในการใช้ระบบงานคอม และเพื่อเป็นการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนในการปฏิบัติงานของเจ้าหน้าที่บริษัท ซึ่งมีหน้าที่ความรับผิดชอบดังนี้

1. กรรมการผู้จัดการบริษัท มีหน้าที่ดังต่อไปนี้
   - 1.1 ดูแลและรับผิดชอบการปฏิบัติหน้าที่ต่างๆ ของเจ้าหน้าที่ทุกคนในบริษัท เพื่อตอบสนองต่อนโยบายบริษัท
   - 1.2 กำหนดนโยบายและหลักการปฏิบัติ
   - 1.3 มีอำนาจอนุมัติในหลักการและค่าใช้จ่ายบริษัท
   - 1.4 ดูแลและติดตามความคืบหน้า และประเมินผลทุกระดับ และทุกฝ่ายในบริษัท เคเอสแอล ไอทีเซ็นเตอร์ จำกัด
   - 1.5 มีอำนาจลงโทษพนักงาน ที่ละเมิดต่อกฎระเบียบต่าง ๆ ของกลุ่มบริษัท ไม่ว่าจะจงใจหรือมิได้จงใจ โดยยึดถือแนวทางการลงโทษตามระเบียบของบริษัท
2. รองกรรมการผู้จักการ มีหน้าที่ดังต่อไปนี้
   - 2.1 ดูแลและรับผิดชอบการปฏิบัติงานต่าง ของเจ้าหน้าที่ทุกคนในสายงานระบบคอมพิวเตอร์ เพื่อตอบสนองต่อนโยบายกลุ่มบริษัท
   - 2.2 มีอำนาจอนุมัติในหลักการและค่าใช้จ่ายในฝ่ายที่รับผิดชอบในวงเงินที่ของบประมาณไว้หรือนำเรื่องเข้าที่ประชุมกรรมการบริษัท เพื่อพิจารณาอนุมัติ
   - 2.3 วางแผนและจดทำงบประมาณภายในส่วนงานระบบคอมพิวเตอร์ เพื่อนำเสนอฝ่ายบริหาร เมื่อได้รับแล้วต้องประสานงานกับทางผู้จัดการฝ่ายต่างๆ เพื่อควบคุมดูแลค่าใช้จ่ายต่างๆ ที่เกิดขึ้นให้สอดคล้องกับงบประมาณที่ได้รับและเกิดประสิทธิภาพสูงสุด
   - 2.4 ดูแลและติดตามความคืบหน้า และประเมินผลงานของทุกระดับ และทุกฝ่าย ในสายงาน
   - 2.5 วิเคราะห์และประเมินผลการทำงานของเจ้าหน้าที่ทุกคน ในสายงาน ปีละ 2 ครั้ง
   - 2.6 ลงโทษพนักงานในสายงานที่รับผิดชอบ ในกรณีที่ทำการละเมิดต่อกฎระเบียบต่าง ๆ ของกลุ่มบริษัท ไม่ว่าจะจงใจหรือมิได้จงใจ โดยยึดถือแนวทางการลงโทษตามกฎระเบียบของบริษัท
3. ผู้จัดการฝ่าย Application Development มีหน้าที่ดังต่อไปนี้
   - 3.1 ดูแลและรับผิดชอบการปฏิบัติหน้าที่ต่างๆ ของเจ้าหน้าที่ทุกคนในฝ่าย Application Development เพื่อตอบสนองต่อนโยบายกลุ่มบริษัท
   - 3.2 วางแผนและจัดการงบประมาณภายในฝ่าย Application Development เพื่อนำเสนอต่อฝ่ายบริหาร เมื่อได้รับงบประมาณแล้วผู้จัดการฝ่าย Application Development จะต้องควบคุมดูแลค่าใช้จ่ายต่างๆ ที่เกินขึ้นสอดคล้องกับงบประมาณที่ได้รับ และเกิดประสิทธิภาพสูงสุด

3.3 ดูแลและติดตามความคืบหน้า และประเมินผลงานการวางระบบต่างๆ เจ้าหน้าที่โครงการทุกคนพร้อมทั้งให้ความช่วยเหลือ ที่จำเป็นต่อความก้าวหน้าของโครงการ

3.4 วิเคราะห์และประเมินผลงานการทำงานของเจ้าหน้าที่ทุกคนในฝ่าย Application Development ปีละ 2 ครั้ง

3.5 ดูและ จัดหาและตระเตรียมเครื่องมืออุปกรณ์ต่าง ๆ ที่จำเป็นภายในฝ่าย Application Development

3.6 ลงโทษพนักงานภายใน Application Development ที่ทำการละเมิดต่อกฎระเบียบต่างๆ ของกลุ่มบริษัท ไม่ว่าจะจงใจหรือมิได้จงใจ โดยยึดถือแนวทางการลงโทษตามกฎระเบียบของกลุ่มบริษัท

4. ผู้ช่วยผู้จัดการฝ่าย Application Development ส่วนพัฒนาระบบคอมพิวเตอร์ มีหน้าที่ดังต่อไปนี้

4.1 ควมคุมและดูแลงานต่างๆ ในส่วนของการพัฒนาระบบงานคอมพิวเตอร์ให้มีหน้าที่ความถูกต้องครบถ้วนและเสร็จทันตามกำหนดเวลาที่ได้ว่างไว้ในแผนงาน

4.2 ควบคุมและดูและการจัดเก็บโปรแกรมต้นฉบับและเวอร์ชั่นต่างๆ ของแต่ละระบบงานคอมพิวเตอร์ที่ใช้ในกลุ่มบริษัท

4.3 ควมคุมและดูแลการจัดเตรียมและจัดเก็บฐานข้อมูลของระบบงานคอมพิวเตอร์ต่างๆ ที่ใช้ในกลุ่มบริษัท

4.4 ออกแบบและจัดทำเอกสารมาตรฐานต่าง ๆ ที่ใช้ในการพัฒนาระบบคอมพิวเตอร์

4.5 ศึกษาและค้นคว้าหาเครื่องมือใหม่ๆ มาช่วยพัฒนาระบบงานคอมพิวเตอร์ให้สะดวกและรวดเร็วยิ่งขึ้น

4.6 พัฒนางานคอมพิวเตอร์และทดสอบโปรแกนมต่างย่อยต่างๆ ตามที่ได้รับงานมาจากส่วนงานที่ปรึกษาระบบ

4.7 วิเคราะห์ประเมินผลการทำงานของเจ้าหน้าที่ทุกคนในส่วนพัฒนาระบบคอมพิวเตอร์ ปีละ 2 ครั้ง

5. ผู้ช่วยผู้จัดการฝ่าย Application Development ส่วนที่ปรึกษาระบบ มีหน้าที่ดังต่อไปนี้

5.1 ควบคุมและดูแลงานต่างๆ ในส่วนของที่ปรึกษาระบบ ทั้งงานส่วนโครงการและงานสนับสนุน ให้มีความถูกต้องครบถ้วนและเสร็จตามกำหนดเวลาที่ได้วางไว้ในแผนงาน

5.2 ควบคุมและดูแลในส่วนของการจัดทำคู่มือและเอกสารต่างๆ ประกอบงานคอมพิวเตอร์

5.3 ควบคุมและดูแลในส่วนของงานจัดอบรมระบบงานคอมพิวเตอร์ต่าง ๆ ในกลุ่มบริษัท

5.4 กำหนดรอบและวางแผนการเข้าไปสำรวจความต้องการต่าง ๆ ของผู้ใช้ระบบงานในแต่ละบริษัท

5.5 ศึกษาและค้นคว้าระบบงานคอมพิวเตอร์ใหม่ที่มีประโยชน์และสร้างมูลค่าเพิ่มมานำเสนอให้กับแต่ละกลุ่มบริษัท

5.6 ออกแบบภาพรวมและรายละเอียด รวมถึงจัดทำเอกสารการแก้ไขระบบงานคอมพิวเตอร์เดิมหรือจัดทำระบบงานคอมพิวเตอร์ใหม่เพื่อส่งมอบงานให้ส่วนงานพัฒนาระบบคอมพิวเตอร์นำไปใช้ในการพัฒนาระบบต่อไป

5.7 วิเคราะห์และประเมินผลการทำงานของเจ้าหน้าที่ทุกคนในส่วนงานที่ปรึกษาระบบปีละ 2 ครั้ง

6. เจ้าหน้าที่ส่วนพัฒนาระบบคอมพิวเตอร์ มีหน้าที่ดังต่อไปนี้

6.1 พัฒนาระบบงานคอมพิวเตอร์และทดสอบโปรแกรมย่อยต่างๆ ให้มีความถูกต้องและครบถ้วนและเสร็จทันตามกำหนดเวลาที่ได้รับงานมาจากส่วนงานที่ปรึกษาระบบ

6.2 จัดเก็บโปรแกรมต้นฉบับและเวอร์ชั่นต่างๆ ของแต่ละระบบงานคอมพิวเตอร์ที่ตนเองรับผิดชอบ

6.3 จัดเตรียมและจัดเก็บฐานข้อมูลของระบบงานคอมพิวเตอร์ให้สะดวกและรวดเร็วยิ่งขึ้น

7. เจ้าหน้าที่ส่วนพัฒนาระบบคอมพิวเตอร์ มีหน้าที่ดังต่อไปนี้

7.1 เก็บและรวบรวมข้อมูล เพื่อศึกษาความต้องการต่างๆ ของผู้ใช้ระบบงานคอมพิวเตอร์อย่างละเอียดถี่ถ้วน

7.2 ออกภาพรวมและรายละเอียด รวมถึงการจัดทำเอกสารในการแก้ไขระบบงานคอมพิวเตอร์เดิมหรือจัดทำระบบงานคอมพิวเตอร์ใหม่เพื่อส่งมอบงานให้ส่วนงานพัฒนาระบบคอมพิวเตอร์นำไปใช้ในการพัฒนาระบบต่อไป

7.3 ทดสอบโปรแกรมทั้งระบบเพื่อตรวจสอบว่าตรงกับความต้องการของผู้ใช้หรือไม่

7.4 ในกรณีที่พบข้อผิดพลาดของโปรแกรม หรือพบว่าไม่ตรงกับความต้องการของผู้ใช้ให้ทำการนัดหมายกับบริษัทผู้ผลิตโปรแกรมหรือส่วนงานพัฒนาระบบคอมพิวเตอร์ เพื่อปรึกษาหารือถึงแนวทางในการแก้ไขปัญหา

7.5 จัดทำคู่มือและเอกสารต่าง ๆ ประกอบระบบงานคอมพิวเตอร์ที่ตัวเองรับผิดชอบ

7.6 จัดเตรียมเอกสารและอุปกรณ์คอมพิวเตอร์ โปรแกรมและฐานข้อมูลที่ตัวเองรับผิดชอบ เพื่อใช้ฝึกอบรมผู้ใช้ระบบงาน

7.7 ทำการฝึกอบรมผู้ใช้ที่เกี่ยวข้องทุกคนในการแก้ไขระบบงานคอมพิวเตอร์เดิมหรือจัดทำระบบงานคอมพิวเตอร์ใหม่

7.8 จัดให้มีการประชุมเป็นระยะๆ อย่างน้อยเดือนละ 2 ครั้งเพื่อติดตามความคืบหน้าและแก้ไขปัญหาได้ทันท่วงที

7.9 ดูแลและให้คำปรึกษาเกี่ยวกับระบบงานคอมพิวเตอร์ต่างๆ แก่ผู้ใช้ในกรณีที่ผู้ใช้เกิดปัญหาการใช้งาน

8. ผู้จัดการฝ่าย Infrastructure มีหน้าที่ดังต่อไปนี้

8.1 ดูแลและรับผิดชอบการปฏิบัติงานต่างๆ ของเจ้าหน้าที่ทุกคนในฝ่าย Infrastructure เพื่อตอบสนองต่อนโยบายกลุ่มบริษัท

8.2 งานแผนและจัดทำงบประมาณในฝ่าย Infrastructure เพื่อนำเสนอต่อฝ่ายบริหารเมื่อได้รับงบประมาณแล้วผู้จัดการฝ่าย Infrastructure จะต้องควบคุมดูแลค่าใช้จ่ายต่างๆ ที่เกิดขึ้นให้สอดคล้องกับงบประมาณที่ได้รับและเกิดประสิทธิภาพสูงสุด

8.3 ดูแลและติดตามความคืบหน้า และประเมินผลงานการวางแผนระบบงานต่างๆ ของเจ้าหน้าที่โครงงานทุกคนพร้อมทั้งให้ความช่วยเหลือต่างๆ ที่จำเป็นต่อความก้าวหน้าของโครงการ

8.4 วิเคราะห์และประเมินผลการทำงานของเจ้าหน้าที่ทุกคนในฝ่าย Infrastructure ปีละ 2 ครั้ง

8.5 ดูแล จัดหา และตระเตรียมเครื่องมืออุปกรณ์ต่าง ๆ ที่จำเป็นภายในฝ่าย Infrastructure

8.6 ลงโทษพนักงานภายในฝ่าย Infrastructure ที่กระทำการละเมิดต่อกฎระเบียบต่างๆ ของกลุ่มบริษัท ไม่ว่าจะจงใจหรือ มิได้จงใจ โดยยึดถือแนวทางการลงโทษตามกฎระบียบของบริษัท

9. ผู้ช่วยผู้จัดการฝ่าย Infrastructure ส่วนระบบเครือข่ายและความปลอดภัย มีดังต่อไปนี้

9.1 ดูแล และจัดหาตระเตรียมอุปกรณ์ Network ในระบบเครือข่ายที่จำเป็นต่างๆ ภายในฝ่าย Infrastructure และบริษัทในกลุ่ม โดยผ่านความเห็นชอบจากผู้จัดการฝ่าย Infrastructure

9.2 บำรุงรักษาอุปกรณ์ Network ในระบบเครือข่าย ให้อยู่ในสภาพที่ใช้งานได้ตลอดเวลา

9.3 วางแผนการสำรองอุปกรณ์ต่าง ๆ ที่จำเป็นเพื่อมิให้ระบบเครือข่ายหยุดชะงัก

9.4 วางแผนและออกแบบเครือข่ายทั้งหมดภายในกลุ่มบริษัท ทั้งปัจจุบันและอนาคตเพื่อความเจริญก้าวหน้าของกลุ่มบริษัท

9.5 กำหนดหมายเลข IP Address แก่เครื่องบริการแม่ข่ายหรือเครื่องลูกข่ายทุกเครื่องภายในบริษัท

9.6 ทำการตรวจสอบระบบเครือข่ายเป็นประจำทุกวันเพื่อทำให้ระบบงานทำงานได้อย่างสม่ำเสมอเป็นปกติ พร้อมทั้งทำการวิเคราะห์และปรับปรุงระบบเครือข่ายให้มีประสิทธิภาพสูงสุด

9.7 ดูแล และจัดเตรียมโปรแกรมระบบป้องกันภัยคุกคามทางระบบคอมพิวเตอร์คอมพิวเตอร์ที่ทันสมัย เพื่อนำมาใช้ในบริษัท และค่อยปรับปรุงให้ทันสมัยอยู่เสมอ

9.8 กำหนดสิทธิการใช้งานระบบ Internet ให้กับผู้ใช้งาน ในกลุ่มบริษัท ตามเอกสารร้องขอใช้งานและผ่านการอนุมัติจากผู้จัดการฝ่ายต่างๆ และได้รับอนุมัติจากผู้จัดการฝ่าย Infrastructure เรียบร้อยแล้ว

9.9 ให้คำแนะนำฝ่ายคอมพิวเตอร์ของบริษัทต่างๆ ในกลุ่ม ให้ใช้ระบบป้องกันภัยคุกคามทางระบบคอมพิวเตอร์คอมพิวเตอร์ตัวเดียวกัน เพื่อเป็นมาตรฐานเดียวกันและเพื่อความมั่นใจว่าระบบเครือข่ายภายในบริษัท จะปลอดภัยจากภัยคุกคามทางระบบคอมพิวเตอร์คอมพิวเตอร์

9.10 ดูแล และจัดเตรียมระบบเครือข่าย Internet และ Intranet เพื่อนำมาใช้ในบริษัทและคอยปรับปรุงให้ทันสมัยอยู่เสมอ

9.11 ดูแล และจัดเตรียมระบบ IP Voice/IP Phone , Video Conference และระบบ CCTV เพื่อนำมาใช้ในบริษัท และคอยปรับปรุงให้ทันสมัยอยู่เสมอ

9.12 ดูและ จัดหา และจัดเตรียมระบบ Network Monitoring เพื่อนำมาใช้ในบริษัท และคอยปรับปรุงให้ทันสมัยอยู่เสมอ

9.13 ในกรณีที่ตรวจพบว่ามีการใช้งานในระบบการสื่อสารผิดปกติ (ถูกโจมตีจากเครื่องคอมพิวเตอร์ทั้งภายในและภายนอก) จะต้องรีบแจ้งเป็นลายลักษณ์อักษร ให้ผู้จัดการฝ่าย Infrastructure หรือรายงานให้กับรองกรรมการผู้จัดการส่วนงานคอมพิวเตอร์ทราบโดยทันที

9.14 ปฏิบัติงานตามที่ได้รับมอบหมายจากผู้บริหาร และดำเนินการแก้ไขปัญหาการทำงานผิดปกติกับระบบเครือข่าย

9.15 ในกรณีที่พบเห็นผู้ใช้งานฝ่าฝืนกฎระเบียบการใช้งานคอมพวเตอร์ ของกลุ่มบริษัท และหรือการละเมิดใช้โปรแกรมที่ผิดกฎหมาย ให้ทำหนังสือเป็นลายลักษณ์อักษรเพื่อแจ้งแก่ผู้จัดการฝ่าย Infrastructure หรือรายงานให้กับรองกรรมการผู้จัดการสายงานระบบปฏิบัติการคอมพิวเตอร์ทราบโดยทันที

10. ผู้ช่วยผู้จัดการฝ่าย Infrastructure ส่วนระบบคอมพิวเตอร์ มีหน้าที่ดังต่อไปนี้

10.1 ดูแล จัดหา และจัดเตรียมระบบงานอีเมล์ให้กับผู้ใช้ทุกคนที่ร้องขอ โดยมีหนังสือเป็นลายลักษณ์อักษรซึ่งผ่านความเห็นชอบจากผู้บัญชาโดยตรง และได้รับการอนุมัติจากผู้จัดการฝ่าย Infrastructure

10.2 กำหนดผู้ใช้และรหัสประจำตัวแก่ผู้ขอใช้ระบบเครือข่ายทุกคนที่ทำเอกสารการขอใช้อย่างถูกต้อง และได้อนุมัติรับจากผู้จัดการฝ่าย Infrastructure

10.3 กำหนดสิทธิการเข้าใช้ฐานข้อมูลของผู้ใช้ทุกคน ตามที่ได้รับการอนุมัติจากผู้บริหารของส่วนงานต่างๆ

10.4 ทำการสำรองของบริษัท ขึ้นระบบ Storage Disk ทุกวันอย่างน้อยวันละ 1 ครั้ง หลังเวลา 24:00 น.เป็นต้นไป เพื่อไม่ให้การทำงานของผู้ใช้หยุดชะงัก

10.5 ทำการสแกนและฆ่าภัยคุกคามทางระบบคอมพิวเตอร์ เครื่องแม่ข่ายเป็นประจำโดยสม่ำเสมอ

10.6 ให้คำแนะนำฝ่ายคอมพิวเตอร์ของบริษัทต่างๆ ในกลุ่มให้ใช้โปรแกรมระบบป้องกันภัยคุกคามทางระบบคอมพิวเตอร์คอมตัวเดียวกัน เพื่อเป็นมาตรฐานเดียวกันและเพื่อความมั่นใจว่าระบบเครื่อข่ายในกลุ่มบริษัท จะปลอดภัยจากภัยคุกคามทางระบบคอมพิวเตอร์

10.7 วางแผนการตรวจสอบและทำการตรวจสอบเพื่อให้มั่นใจ ได้ว่าระบบสำรองข้อมูลที่สำรองไว้สามารถนำมาใช้งานได้เมื่อต้องการ

10.8 จัดเตรียมระบบคอมพิวเตอร์แม่ข่ายสำหรับโครงการต่างๆ ในอนาคตกรณีที่หัวหน้าโครงการร้องขอเป็นลายลักษณ์อักษรผ่านทางรองกรรมการผู้จัดการสายงานระบบปฏิบัติการคอมพิวเตอร์

10.9 ในกรณีเครือแม่ข่ายมีปัญหา ผู้ช่วยผู้จัดการฝ่าย ส่วนระบบคอมพิวเตอร์จะต้องรีบแจ้งให้ผู้จัดการฝ่าย Hardware, ผู้จัดการฝ่าย Software และหัวหน้าโครงการนั้นๆ ทราบโดยทันทีเพื่อทำการปรึกษาหารือเพื่อหาทางแก้ไข และปรับย้าย ระบบงานหรือฐานข้อมูลที่มีปัญหานั้นๆ ไปยังเครื่อแม่ข่ายสำรอง และเมื่อได้ข้อสรุปแล้ว จะต้องรีบดำเนินการแก้ไขปัญหาจนเป็นปกติทันที

11. เจ้าหน้าที่ดูแลระบบฐานข้อมูล มีหน้าที่ดังต่อไปนี้

11.1 ติดตั้ง Configuration Database Serverของฐานข้อมูลระบบงานคอมพิวเตอร์ต่างๆ ที่ใช้ในกลุ่มบริษัท

11.2 Set Up Job Replicate Data และ Job maintenance Database ของฐานข้อมูลระบบงานคอมพิวเตอร์ต่างๆ

11.3 ตรวจสอบและดูแล Job ต่างๆ บน Database Server ให้อยู่ในสภาพปกติ เป็นประจำทุกวันโดยสม่ำเสมอ

11.4 ตรวจสอบและดูแลพื้นที่ที่ว่างบน Database Server เพื่อให้สามารถ Backup ฐานข้อมูลได้ทุกๆ วัน

11.5 วางแผนการตรวจสอบและทำการตรวจสอบทุกๆ 3 เดือน เพื่อให้มั่นใจได้ว่าฐานข้อมูลที่สำรองไว้สามารถนำมาใช้งานได้เมื่อต้องการ

11.6 วิเคราะห์และแก้ไขปัญหาต่างๆ ที่เกิดขึ้นกับ Database Server ของฐานข้อมูลระบบงานคอมพิวเตอร์ต่างๆ

11.7 ในกรณีข้อมูลมีปัญหา ผู้ดูแลระบบงานฐานข้อมูลต้องรีบแจ้งให้ผู้จัดการฝ่าย Software และหัวหน้าโดยโครงการนั้นๆ ทราบโดยทันทีเพื่อทำการปรึกษาหารือหารือเพื่อหาทางแก้ไขฐานข้อมูลที่มีปัญหานั้นๆ และเมื่อได้ข้อสรุปแล้วผู้บริหารฐานข้อมูลต้องรีบดำเนิดงานจนเป็นปกติทันที

11.8 ควบคุมและดูแลในส่วนระบบรักษาความปลอดภัยบน Database Server ของฐานข้อมูลระบบงานคอมพิวเตอร์ต่างๆ

11.9 ในกรณีที่ผู้เข้าใช้งานฐานข้อมูลโดยมิได้รับอนุญาตไม่ว่าจะตั้งใจหรือมิได้ตั้งใจ และไม่ว่าโดยวิธีใดผู้ดูแลระบบฐานข้อมูลจะต้องทำหนังสือตักเตือนไปยังผู้บังคับบัญชาของผู้นั้นโดยทันที และทำหนังสือเป็นลายลักษณ์อักษรแจ้งผู้ที่จัดการฝ่าย Software ทราบ

11.10 ควบคุมและดูแลในส่วนของการจัดทำคู่มือและเอกสารต่างๆ ประกอบการดูแล Database Server

11.11 ศึกษาและค้นคว้าเทคโนโลยีใหม่เกี่ยวกับฐานข้อมูลเพื่อนำมาประยุคต์ใช้ในกลุ่มบริษัท

12. เจ้าหน้าที่ส่วนระบบเครือข่ายและความปลอดภัย มีหน้าที่ต้องปฏิบัติดังนี้

12.1 ทำหนังสือเป็นลายลักษณ์อักษรในกรณีที่ผู้ใช้คนใดคนหนึ่งหรือหลายคน ได้กระทำการฝ่ายฝืนกฎระเบียบการใช้งานคอม ทั้งที่ตั้งใจและมิได้ตั้งใจให้พนักงานท่านนั้นหรือเหล่านั้นทราบ

12.2 กำหนดสิทธิการใช้งานระบบ Internet ให้กับผู้ใช้งาน ในกลุ่มบริษัท ที่ทำเอกสารร้องขอใช้งานและผ่านการอนุมัติจากผู้จัดการฝ่ายต่างๆ และได้รับอนุมัติจากผู้จัดการฝ่าย Infrastructure เรียบร้อยแล้ว

12.3 ดูและและตรวจสอบระบบการสื่อสารข้อมูลระหว่าง Site ต่างๆ ให้อยู่ในสภาพปกติเป็นประจำทุกวัน โดยสม่ำเสมอ

12.4 ในกรณีที่ตรวจพบว่ามีการใช้งานในระบบการสื่อสารผิดปกติ (ถูกโจมตีจากเครื่องคอมพิวเตอร์ทั้งภายในและภายนอก) จะต้องรีบแจ้งเป็นลายลักษณ์อักษร ให้ผู้จัดการฝ่าย Infrastructure หรือรายงานให้กับรองกรรมการผู้จัดการส่วนงานคอมพิวเตอร์ทราบโดยทันที

12.5 ปฏิบัติงานตามที่ได้รับมอบหมายจากผู้ช่วยผู้จัดการส่วนระบบเครือข่ายและความปลอดภัย พร้อมทั้งแก้ไขการทำงานที่ผิดปกติในระบบเครือข่าย ที่ได้รับมอบหมายให้ดำเนินการแก้ไข

12.6 ในกรณีที่พบเห็นผู้ใช้งานฝ่าฝืนกฎระเบียบการใช้งานคอมพิวเตอร์ของกลุ่มบริษัท และหรือการละเมิดใช้โปรแกรมที่ผิดกฎหมาย ให้ทำหนังสือเป็นลายลักษณ์อักษรเพื่อแจ้งแก่ผู้ช่วยผู้จัดการฝ่ายส่วนระบบเครือข่ายและความปลอดภัย และผู้จัดการฝ่าย Infrastructure หรือรายงานให้กับรองกรรมการผู้จัดการส่วนระบบคอมพิวเตอร์ ทราบโดยทันที

12.7 ช่วยดูแล จัดหา อุปกรณ์ หรือโปรแกรมเพื่อดูแล รักษาความปลอดภัยในระบบเครือข่าย ให้พร้อมใช้งานและทันสมัยอยู่เสมอ

13. เจ้าหน้าที่งานบริหารส่วนระบบคอมพิวเตอร์ มีหน้าที่ต้องปฏบัติดังนี้

13.1 ดำเนินการติดตั้งระบบคอมให้กับผู้ใช้ทุกคนในกลุ่มบริษัท ที่ทำเอกสารร้องขอการใช้งานและผ่านการอนุมัติจากผู้จัดการฝ่าย Infrastructure และหรือ ผู้ช่วยผู้จัดการฝ่าย ส่วนระบบคอมพิวเตอร์ เรียบร้อยแล้ว

13.2 ทำการกำหนดค่าต่างๆ ในระบบคอม ตามที่ได้รับมอบหมายจากผู้จัดการฝ่าย ส่วนระบบเครือข่ายหรือผู้ช่วยผู้จัดการฝ่าย ส่วนระบบคอมพิวเตอร์

13.3 ดูแล พร้อมแก้ไขปัญหา เครื่องคอมพิวเตอร์ ในระบบเครือข่ายให้สามารถใช้งานได้ตามปกติ

13.4 ทำการสแกน และฆ่าภัยคุกคามทางระบบคอมพิวเตอร์คอมในระบบเครื่อข่ายเป็นประจำโดยสม่ำเสมอ

13.5 ปฏิบัติงานตามที่ได้รับมอบหมายจากผู้บังคับบัญชา ในการแก้ไขการทำงานผิดปกติของระบบคอมพิวเตอร์ และอุปกรณ์ในระบบเครื่อข่าย

13.6 ดูแล และทำการบำรุงรักษา อุปกรณ์สำรองระบบกระสไฟฟ้า UPS / Generator