บริษัท แอ็พพลาย ดีบี จำกัด (มหาชน)

APPLIED DB PUBLIC COMPANY LIMITED

นโยบายการรักษาความมั่นคงปลอดภัย ของระบบสารสนเทศ (Information System Security Policy)

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information System Security Policy)

ปัจจุบันมีการขับเคลื่อนด้วยเทคโนโลยี ภัยคุกคามทางไซเบอร์จึงกลายเป็นปัญหาที่ท้าทายและหลีกเลี่ยงได้ยากสำหรับองค์กรทุกขนาด นโยบายความมั่นคงปลอดภัยของสารสนเทศที่แข็งแกร่งและมีประสิทธิภาพ จึงเป็นเสมือนเกราะป้องกันที่สำคัญ ช่วยปกป้องข้อมูลสำคัญ สร้างความเชื่อมั่นให้กับลูกค้าและเสริมสร้างความมั่นคงให้กับธุรกิจ

บริษัท แอ็พพลาย ดีบี จำกัด (มหาชน) และบริษัทย่อย ได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ จึงมีการสร้างความรู้และความตระหนักในการใช้งานระบบสารสนเทศอย่างมั่นคงปลอดภัยแก่ผู้ใช้งาน ผู้ปฏิบัติงาน โดยการจัดทำนโยบายและเผยแพร่เอกสารที่เกี่ยวข้องผ่านระบบ Intranet ภายในขององค์กร รวมถึงสื่อสารนโยบายความมั่นคงปลอดภัยของระบบสารสนเทศให้ผู้ให้บริการภายนอกทราบในเรื่องที่เกี่ยวข้อง รวมถึงการสรรหาบุคลากร ต้องเป็นไปตามเกณฑ์ที่กำหนดและมีการตรวจสอบคุณสมบัติ (Screening) ของผู้สมัครงานทุกคน รวมทั้งตรวจสอบประวัติอาชญากรรมจากสำนักงานตำรวจแห่งชาติ ตลอดจนจัดทำข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment) ให้เป็นไปตามเกณฑ์ที่กำหนด

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องในบริษัท แอ็พพลาย ดีบี จำกัด (มหาชน) และบริษัทย่อย ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ สำหรับแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ มีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบายและการปฏิบัติตามนโยบาย

บริษัทฯ ตระหนักถึงความมั่นคงปลอดภัยของระบบสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายความมั่นคงปลอดภัยระบบสารสนเทศฉบับนี้ เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในบริษัทฯ รวมทั้งเป็นมาตรการป้องกันความเสี่ยงของปัญหาที่อาจจะเกิดขึ้นและเพื่อให้สอดคล้องกับนโยบายความปลอดภัยของบริษัทฯ ด้านอื่นๆ ที่มุ่งเน้นการปฏิบัติงานภายในบริษัทฯ ให้มีความมั่นคงปลอดภัย ดังนี้

1) เพื่อใช้เป็นแนวทางในการจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศให้เป็นไปตามมาตรฐานสากล
2) เพื่อส่งผลให้ระบบสารสนเทศมีความมั่นคงปลอดภัยและมีประสิทธิภาพ
3) เพื่อให้ฝ่ายบริหารและฝ่ายปฏิบัติการ เข้าใจหลักการและกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
4) เพื่อให้มีการปฏิบัติตามกระบวนการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นระบบและต่อเนื่อง
5) เพื่อเป็นเครื่องมือสื่อสารและสร้างความเข้าใจตลอดจนเชื่อมโยงนโยบายความมั่นคงปลอดภัยระบบสารสนเทศกับกลยุทธ์ของบริษัทฯ
6) เพื่อใช้เป็นเครื่องมือในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องและให้เจ้าหน้าที่ทุกระดับในบริษัทฯ บุคคลที่เกี่ยวข้องถือปฏิบัติอย่างเคร่งครัด

2. ขอบเขตของการสร้างความมั่นคงปลอดภัย

นโยบายฉบับนี้มีขอบเขตครอบคลุมถึงการสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศต่างๆ ของบริษัทฯ ดังนี้

1) พนักงานและลูกจ้างของบริษัทฯทั้งหมด
2) ข้อมูล/สารสนเทศของบริษัทฯ
3) เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ ของบริษัทฯ
4) เครื่องคอมพิวเตอร์ส่วนบุคคล
5) เครื่องคอมพิวเตอร์แบบพกพา
6) อุปกรณ์เครือข่าย

7) ระบบไฟฟ้าสำรอง
8) สายสัญญาณเครือข่าย
9) ซอฟท์แวร์ระบบ ซอฟท์แวร์จ้างพัฒนา ซอฟท์แวร์พัฒนาเอง ซอฟท์แวร์สำเร็จรูป
10) สื่อบันทึกข้อมูล
11) เอกสารของบริษัทฯ

3. นิยามและคำจำกัดความที่สำคัญ

1) **"บริษัท"** หมายถึง บริษัท แอ็พพลาย ดีบี จำกัด (มหาชน) และบริษัทย่อย
2) **"ผู้บริหารระดับสูง"** หมายถึง ประธานเจ้าหน้าที่บริหาร ผู้บริหารที่มีหน้าที่บริหารและกำหนดวัตถุประสงค์ขององค์กร กำหนดกลยุทธ์ กำหนดนโยบายและวางแผนระยะยาว รวมถึงการตัดสินใจแก้ไขปัญหาต่างๆ ที่มีความสำคัญต่างๆ ที่เกี่ยวข้องกับองค์กร
3) **"ฝ่ายเทคโนโลยีสารสนเทศ"** หมายถึง ส่วนงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และระบบเครือข่ายภายในบริษัทฯ
4) **"ผู้อำนวยการและ/หรือผู้ช่วยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ"** หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของบริษัทฯ ให้มีประสิทธิภาพสูงสุด รวมไปถึงนโยบายต่างๆ การวางแผนและการพัฒนา
5) **"ระบบคอมพิวเตอร์"** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
6) **"ระบบเครือข่าย"** หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ถูกนำมาเชื่อมต่อกันผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยนและใช้อุปกรณ์ต่างๆ ของเครือข่ายร่วมกัน
7) **"ระบบสารสนเทศ"** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารทั้งมีสายและไร้สาย ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ
8) **"ระบบอีอาร์พี (ERP System)"** หมายถึง ระบบงานหลักของบริษัทฯ ที่ประกอบการทำงาน ได้แก่ งานด้านบัญชี การเงิน งานด้านการขาย งานด้านการผลิต งานด้านคลังสินค้างานด้านจัดซื้อหรืออื่นๆ ที่เกี่ยวข้อง
9) **"ผู้มีอำนาจ"** หมายถึง ผู้อำนวยการและ/หรือผู้ช่วยผู้อำนวยการฝ่ายของส่วนงานที่มีระบบคอมพิวเตอร์ของบริษัทฯ อยู่ในความครอบครองและให้หมายความรวมถึงผู้ซึ่งได้รับมอบหมายจากบุคคลดังกล่าวด้วย
10) **"ผู้ใช้งาน"** หมายถึง ลูกจ้าง เจ้าหน้าที่ ผู้ดูแลระบบ ผู้บริหารของบริษัทฯ ผู้รับบริการหรือผู้ที่หน่วยงานอนุญาตให้ใช้ระบบคอมพิวเตอร์ได้
11) **"ผู้ดูแลระบบ"** หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
12) **"บัญชีผู้ใช้งาน"** หมายถึง บัญชีผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ
13) **"สิทธิ์ของผู้ใช้งาน"** หมายถึง สิทธิ์ในการเข้าถึงระบบปฏิบัติการ สิทธิ์การใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิ์การใช้งานเครือข่าย รวมถึงสิทธิ์ที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทฯ
14) **"ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)"** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งการห้ามปฏิเสธความรับผิด (Nonrepudiation)
15) **"ความเสี่ยง (Risk)"** หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ความสูญเปล่าหรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

16) **"ปัจจัยเสี่ยง (Risk Factor)"** หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและเกิดขึ้นได้อย่างไร ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

17) **"การประเมินความเสี่ยง (Risk Assessment)"** หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของบริษัทฯ รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

18) **"การบริหารความเสี่ยง (Risk Management)"** หมายถึง กระบวนการจัดการความเสี่ยง ประกอบด้วยกระบวนการในการวิเคราะห์ (Risk Analysis) ประเมินความเสี่ยง (Risk Assessment) ดูแลตรวจสอบและควบคุมความเสี่ยงที่สัมพันธ์กับภารกิจหน้าที่และกระบวนการทำงาน เพื่อให้บริษัทฯ ลดความเสียหายจากความเสี่ยงมากที่สุด

19) **"โปรแกรมประสงค์ร้าย (Malware)"** หมายถึง โปรแกรมคอมพิวเตอร์ชุดคำสั่งและหรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหาย ไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

4. รายละเอียดและเนื้อหา

4.1 <u>ความมั่นคงปลอดภัยสำหรับสารสนเทศและแนวทางในการรักษาความปลอดภัย</u>

ความมั่นคงปลอดภัยสำหรับสารสนเทศ หมายถึง การสร้างความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศ เพื่อป้องกันความเสียหายที่มีต่อองค์ประกอบทางด้านความมั่นคงปลอดภัย 3 ส่วน ดังนี้

1) Confidentiality บริษัทมั่นใจได้ว่าทรัพย์สินในระบบสารสนเทศจะสามารถเข้าถึงได้โดยบุคคลที่ได้รับอนุญาตแล้วเท่านั้น
2) Integrity ทรัพย์สินในระบบสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์พร้อมใช้งานได้ตลอดเวลาโดยไม่มีวันหยุด
3) Availability ทรัพย์สินในระบบสารสนเทศจะต้องสามารถเข้าถึงได้เมื่อมีความจำเป็นที่ต้องใช้งาน บริษัทฯจะต้องกำหนดมาตรการเพื่อรักษาความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศ โดยบริษัทฯจะใช้แนวทางในการดำเนินงานในส่วนรายละเอียดข้อถัดไปในการรักษาความมั่นคงปลอดภัย

4.2 <u>นโยบายความมั่นคงปลอดภัย</u>

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยเกี่ยวกับระบบสารสนเทศของบริษัทฯ ให้เป็นไปตามหรือสอดคล้องกับพันธกิจและระเบียบปฏิบัติที่เกี่ยวข้อง การจัดให้มีนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงป ลอดภัยด้านระบบสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ รวมถึงแนวปฏิบัติในการควบคุม ความเสี่ยงด้านต่าง ๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

นโยบายความมั่นคงปลอดภัย (Security Policy) ซึ่งจะประกอบด้วยระเบียบปฏิบัติต่าง ๆ ที่พนักงาน ต้องปฏิบัติตามโดยเคร่งครัดครอบคลุมนโยบาย 8 ด้าน ดังนี้

1) นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
2) การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)
3) การควบคุมการเข้าออกห้องเซิร์ฟเวอร์ (Server Room) และการป้องกันความเสียหาย (Physical Security)
4) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย (Information and Network Security)
5) การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
6) การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
7) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)

8) การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

4.3 <u>สาระสำคัญของนโยบาย</u>

1) **นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ**

บริษัทฯ ต้องจัดทำนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อป้องกันและรับมือกับผลกระทบที่อาจเกิดขึ้น โดยประเมินถึงความเสี่ยงของข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการประกาศใช้นโยบายนี้เพื่อให้พนักงานตระหนักและปฏิบัติตามนโยบายที่กำหนดไว้

- **<u>วัตถุประสงค์</u>** เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
- **<u>ผู้รับผิดชอบ</u>** ผู้บริหารระดับสูงและผู้จัดการแผนกเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย
- **<u>วิธีปฏิบัติงาน</u>**
  1) จัดให้มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและมีการปรับปรุงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เมื่อมีการเปลี่ยนแปลงให้สอดคล้องกับการปฏิบัติงานและนโยบายดังกล่าวต้องได้รับการอนุมัติจากผู้มีอำนาจที่ได้มอบหมายไว้
  2) จัดทำนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้ง่าย
  3) จัดให้มีการสร้างความตระหนักที่เกี่ยวข้องกับภัยคุกคามทางอินเทอร์เน็ตใหม่ๆ เพื่อให้พนักงานของบริษัทฯ มีความรู้ความเข้าใจและสามารถป้องกันข้อมูลของตนได้ในระดับหนึ่ง อย่างน้อยปีละ 1 ครั้ง
  4) จัดให้มีการทำรายงานสรุปปัญหาและแนวทางแก้ไขที่มีระดับความสำคัญสูง เช่น ปัญหาการใช้เครือข่าย การติดไวรัส โครงการพัฒนาระบบงาน ปัญหาจากผู้ใช้งานและเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศ และปัญหาอื่นๆ ที่เกี่ยวข้อง โดยประมาณเดือนละ 1 ครั้งหรือตามความเหมาะสม
  5) จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศของบริษัทฯ ปีละ 1 ครั้ง และจัดทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ
  6) จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ปีละ 1 ครั้ง และจัดทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ
  7) จัดให้มีการวางแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศเพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัทฯ ทั้งแผนระยะสั้นและแผนระยะยาว

2) **การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)**

บริษัทฯ ต้องจัดให้มีการแบ่งแยกหน้าที่และกำหนดขอบเขตการปฏิบัติงานของพนักงานภายในแผนกเทคโนโลยีสารสนเทศอย่างชัดเจน เพื่อให้สามารถยืนยันการปฏิบัติงานและมีการอนุมัติการปฏิบัติงานอย่างเพียงพอและเหมาะสม และจัดให้มีการตรวจสอบผลการทำงาน เพื่อควบคุมให้การปฏิบัติงานเป็นไปตามนโยบายที่ได้กำหนดไว้

- **<u>วัตถุประสงค์</u>** เพื่อควบคุมความปลอดภัยในการเข้าถึงข้อมูล โดยจัดให้มีการตรวจสอบและอนุมัติการปฏิบัติงานของพนักงานภายในแผนกเทคโนโลยีสารสนเทศให้เป็นไปตามที่กำหนดไว้ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure Risk
- **<u>ผู้รับผิดชอบ</u>** ผู้ช่วยผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย
- **<u>วิธีปฏิบัติงาน</u>**
  1) จัดให้มีการแบ่งแยกหน้าที่ของพนักงานในส่วนการพัฒนาระบบงาน (Developer) ออกจากพนักงานที่ทำหน้าที่บริหารระบบ (System administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง
  2) ต้องจัดให้มีใบกำหนดหน้าที่งานของแต่ละตำแหน่งงานไว้อย่างชัดเจน ซึ่งตำแหน่งงานที่กำหนดไว้เป็นไปตามหลักการแบ่งแยกหน้าที่งานตามข้อ 1 และพนักงานได้รับทราบถึงขอบเขตและหน้าที่การปฏิบัติงานของตนตามที่ได้กำหนดไว้

3) จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการและวัตถุดิบที่พอเพียงต่อการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับในแต่ละปี

4) จัดให้มีการอบรมเพิ่มทักษะและพัฒนาความรู้ความสามารถของพนักงานแผนกเทคโนโลยีสารสนเทศให้เหมาะสม รวมทั้งจัดให้มีการเก็บข้อมูลการฝึกอบรมเหล่านั้นและการประเมินผลการอบรม

3) **การควบคุมการเข้าออกห้องเซิร์ฟเวอร์ (Server Room) และการป้องกันความเสียหาย (Physical Security)**

การควบคุมการเข้าออกห้องเซิร์ฟเวอร์ (Server Room) อย่างเพียงพอ จะเป็นการป้องกันความเสียหาย ซึ่งเกิดจากตัวบุคคลที่ไม่ได้รับอนุญาตหรือเกิดจากอุปกรณ์ ระบบต่างๆ เช่น ระบบไฟฟ้า ระบบอุณหภูมิและความชื้น ดังนั้น บริษัทฯ ต้องมีการควบคุมเพื่อให้สามารถระบุตัวตนของผู้เข้าถึงห้องเซิร์ฟเวอร์ (Server Room) ได้ และการเข้าถึงดังกล่าวต้องได้รับอนุญาตจากผู้จัดการแผนกเทคโนโลยีสารสนเทศ ซึ่งจำกัดไว้เฉพาะบุคคลที่จำเป็นเท่านั้น รวมทั้งการควบคุมให้มีระบบป้องกันความเสียหายที่อาจจะเกิดขึ้น เช่น การป้องกันไฟไหม้หรือไฟฟ้าขัดข้อง

- **<u>วัตถุประสงค์</u>** เพื่อป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (Availability Risk) ส่วนการป้องกันความเสียหาย มีวัตถุประสงค์เพื่อป้องกันให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (Availability Risk)
- **<u>ผู้รับผิดชอบ</u>** เจ้าหน้าที่ส่วนสนับสนุนเทคโนโลยีสารสนเทศ
- **<u>วิธีปฏิบัติงาน</u>**

1) จัดให้มีการประเมินความเสี่ยงทางกายภาพของพื้นที่จัดเก็บอุปกรณ์ที่สำคัญของระบบเทคโนโลยีสารสนเทศ ทั้งที่สำนักงานใหญ่ สถานที่สำรองข้อมูลและจัดทำแผนเพื่อปรับปรุงความเสี่ยงหรือปัญหาที่พบ

2) จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในห้องเซิร์ฟเวอร์ (Server Room) หรือพื้นที่หวงห้ามซึ่งปิดล็อคตลอดเวลา และต้องกำหนดสิทธิ์การเข้าออกห้องเซิร์ฟเวอร์ (Server Room) ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง

3) ต้องมีระบบเก็บบันทึกการเข้าออกห้องเซิร์ฟเวอร์ (Server Room) โดยบันทึกดังกล่าว ต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวโดยผู้จัดการแผนกหรือผู้ที่ได้รับมอบหมายอย่างสม่ำเสมอ

4) ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องเซิร์ฟเวอร์ (Server Room) ต้องมีการอนุมัติจากผู้จัดการแผนกเทคโนโลยีสารสนเทศก่อนและให้มีเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศที่ปฏิบัติงานประจำในห้องเซิร์ฟเวอร์ (Server Room) ควบคุมดูแลตลอดเวลาระหว่างที่บุคคลดังกล่าวอยู่ในห้องเซิร์ฟเวอร์ (Server Room)

5) ห้องเซิร์ฟเวอร์หลัก (Main Server Room) ต้องมีระบบแจ้งเตือนอัคคีภัย ระดับตรวจวัดอุณหภูมิ สำหรับห้องเซิร์ฟเวอร์ (Server Room) และถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

6) มีการติดตั้งอุปกรณ์สำรองไฟสำหรับระบบคอมพิวเตอร์ เพื่อความต่อเนื่องของระบบงานที่สำคัญ

7) ต้องมีการควบคมอุณหภูมิและความชื้น ให้เหมาะสมกับระบบคอมพิวเตอร์และกำหนดระดับอุณหภูมิและความชื้นที่เหมาะสม

4) **การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย (Information and Network Security)**

บริษัทฯ ต้องควบคุมความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลของบริษัทฯ ตั้งแต่ระดับข้อมูลทั่วไปจนถึงระดับข้อมูลที่ลับที่สุดและควรจะมีหน่วยงานที่ทำหน้าที่ควบคุมหรืออนุมัติการเผยแพร่ข้อมูลข่าวสารให้กับฝ่ายงานอื่นๆ หรือนำข้อมูลออกไปเผยแพร่ภายนอกบริษัทฯ อาจทำให้มีการนำข้อมูลไปใช้โดยไม่ได้รับอนุญาตหรือส่งผลเสียต่อการดำเนินงานของบริษัทฯ ดังนั้น วิธีการปฏิบัติงานอย่างเพียงพอจะช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

■ **<u>วัตถุประสงค์</u>** เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไขเปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ ในส่วนที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่าย มีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ ไม่ให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์เครื่องแม่ข่ายและระบบเครือข่าย

4.1) <u>ความปลอดภัยของข้อมูล</u>

■ **<u>ผู้รับผิดชอบ</u>**

1) **<u>ข้อมูลด้าน IT</u>** (ข้อมูลด้านการจัดการ IT จัดการโครงการ งบประมาณการพัฒนา/บำรุงรักษาระบบ)
   - **ข้อมูลทั่วไป** ดูแลโดยส่วนงาน/ผู้ที่ได้รับมอบหมาย ใช้งานหรือดูแลข้อมูลนั้น ๆ
   - **ข้อมูลลับ** ดูแลโดยส่วนงานที่มีหน้าที่รับผิดชอบและหน้าที่ที่กำหนดในโครงสร้างของฝ่ายหรือผู้ที่ได้รับมอบหมาย ให้ปฏิบัติงานในเรื่องนั้น ๆ
2) **<u>ข้อมูลของบริษัทฯ/ฝ่ายที่อยู่ในระบบ IT</u>** (ข้อมูลที่ใช้ในการดำเนินงานของบริษัทฯ ทั้งด้านการให้บริการธุรกรรมต่างๆ และข้อมูลเพื่อการบริหารจัดการที่อยู่ในระบบ IT โดยแผนกเทคโนโลยีสารสนเทศให้การสนับสนุนการใช้งานจัดเป็นข้อมูลที่มีความสำคัญ)
   - ข้อมูลที่ใช้งานในการดำเนินงานของบริษัทฯ ดูแลโดยบุคคลหรือส่วนงานที่บริษัทฯ กำหนด
   - ข้อมูลที่อยู่ระหว่างประมวลผล ดูแลดยแผนกเทคโนโลยีสารสนเทศ
   - ข้อมูลที่จัดเก็บสำรองตามข้อปฏิบัติด้านระบบ ดูแลโดยแผนกเทคโนโลยีสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) การขอใช้ข้อมูลทุกประเภท ต้องระบุผู้ขอ วัตถุประสงค์และระยะเวลาในการใช้งานที่ชัดเจน
   - การคืนข้อมูล (ถ้ามี) ให้นำมาคืนเมื่อใช้งานเสร็จหรือเมื่อครบกำหนด
   - การยกเลิก (ปิด) สิทธิ์การใช้ข้อมูลให้ยกเลิกเมื่อเสร็จ หรือเมื่อครบกำหนด
   - ห้ามทำสำเนาข้อมูลที่ระบุไว้ว่า “ห้ามทำสำเนา” โดยมิได้รับอนุญาตจากเจ้าของข้อมูล
   - ผู้ขอข้อมูลต้องปฏิบัติตามขั้นตอนการขอใช้ข้อมูลที่กำหนดแตกต่างกันตามประเภทข้อมูลและกลุ่มผู้ขอ
2) กำหนดชั้นความลับของข้อมูลเป็นข้อมูลทั่วไปและข้อมูลลับ และกำหนดวิธีการขอใช้ข้อมูลไว้ดังนี้

   2.1) ข้อมูลทั่วไป คือ ข้อเท็จจริงที่แสดงถึงลักษณะ สถานะหรือเหตุการณ์ต่างๆ โดยอยู่ในรูปแบบที่เหมาะสมในการใช้สื่อสาร แปลความหมายและประมวลผล ซึ่งอาจทำด้วยคนหรือคอมพิวเตอร์ ตัวอย่างลักษณะของข้อมูล เช่น ตัวอักษร ตัวเลข รูปภาพ อีเมล์ สี สัญลักษณ์ รูปทรง อุณหภูมิ ตัวโน๊ตและเสียง ตัวอย่างข้อมูลที่เก็บในรูปแบบต่างๆ
   - ผู้ขอใช้ข้อมูลเป็นพนักงานในแผนก/ฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดกับผู้ดูแลข้อมูล
   - ผู้ขอใช้ข้อมูลเป็นพนักงานนอกแผนก/ฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอแจ้งรายละเอียดเพื่อขออนุมัติจากผู้จัดการแผนก ผู้ดูแลข้อมูล เมื่อได้รับอนุมัติแล้ว จึงแจ้งให้เจ้าหน้าที่ผู้ดูแลข้อมูล จัดทำหรือส่งข้อมูลให้

   2.2) ข้อมูลลับ คือ ข้อมูลที่ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลข้อมูลของหน่วยงานขององค์กรหรือรัฐและเอกชนไม่ให้เผยแพร่โดยไม่ได้รับอนุญาต
   - ผู้ขอใช้เป็นพนักงานในแผนก/ฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอต้องแจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชา (ระดับผู้จัดการแผนก) เมื่อได้รับอนุมัติ แจ้งให้เจ้าหน้าที่ผู้ดูแล จัดทำหรือส่งข้อมูลให้
   - ผู้ขอใช้เป็นพนักงานนอกแผนก/ฝ่ายที่เป็นเจ้าของข้อมูล ผู้ขอต้องแจ้งรายละเอียดเพื่อขออนุมัติจากผู้จัดการแผนกของตนและผู้จัดการแผนกผู้ดูข้อมูลแลตามลำดับ เมื่อได้รับอนุมัติแล้ว จึงแจ้งให้เจ้าหน้าที่ผู้ดูแลจัดทำหรือส่งข้อมูลให้

- ผู้ขอใช้เป็นบุคคลภายนอกหรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้น ๆ แล้วแต่กรณี ให้ตรวจสอบสัญญาหรือเอกสารที่แสดงถึงเป็นผู้ที่ได้รับมอบหมายจากบุคคลภายนอกให้ดำเนินการดังกล่าว จึงพิจารณาการดำเนินการต่อไป โดยผู้พิจารณาอนุมัติต้องเป็นผู้บริหารระดับสูง/ผู้อำนวยการและ/หรือผู้ช่วยผู้อำนวยการฝ่ายขึ้นไป

2.3) ข้อมูลของบริษัท/ฝ่ายที่อยู่ในระบบ IT

- ผู้ขอใช้เป็นพนักงานบริษัทฯ แจ้งรายละเอียดเพื่อขออนุมัติจากผู้บังคับบัญชา (ระดับผู้อำนวยการและ/หรือผู้ช่วยผู้อำนวยการฝ่ายขึ้นไป)
- ผู้ขอใช้เป็นบุคคลภายนอก ให้แจ้งรายละเอียดขอใช้ข้อมูลที่สำนักควบคุมภายในหรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี โดยผู้พิจารณาอนุมัติ ต้องเป็นผู้บริหารระดับสูง/ผู้อำนวยการและ/หรือผู้ช่วยผู้อำนวยการฝ่ายขึ้นไปเมื่อได้รับอนุมัติจากสำนักควบคุมภายในหรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกแล้ว ให้ส่งเรื่องขอใช้ข้อมูลไปยังแผนกเทคโนโลยีสารสนเทศ ผู้ดูแลข้อมูลของแผนกเทคโนโลยีสารสนเทศ พิจารณาอนุมัติให้ใช้ข้อมูลได้ ผู้ดูแลข้อมูลจะสั่งการตามสายงานเพื่อให้เจ้าหน้าที่ผู้ดูแลจัดทำหรือส่งข้อมูล หรือเปิดระบบให้ใช้ข้อมูล (ตามแต่วัตถุประสงค์ของผู้ขอ)
- กรณีผู้ขอใช้ เป็นบุคคลภายนอก หรือหน่วยงานที่ได้รับมอบหมายให้ติดต่อกับบุคคลภายนอกนั้นๆ แล้วแต่กรณี เพื่อดำเนินการติดต่อกับผู้ขอใช้ (บุคคลภายนอก) ให้ตรวจสอบสัญญาหรือเอกสารที่แสดงถึงเป็นผู้ที่ได้รับมอบหมายจากบุคคลภายนอกให้ดำเนินการดังกล่าว จึงพิจารณาการดำเนินการ ต่อไป
- เมื่อครบระยะเวลาใช้งาน หรือผู้ใช้แจ้งใช้งานเสร็จสิ้น (ก่อนครบกำหนด) ผู้ดูแลข้อมูลดำเนินการปิดระบบการเข้าใช้งาน

2.4) การรับส่งข้อมูลสำคัญ ผ่านเครือข่ายสาธารณะต้องเข้ารหัส (encryption) ควบคุมโดยเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศทุกครั้ง

4.2) <u>การควบคุมการกำหนดสิทธิ์และบัญชีรายชื่อผู้ใช้งาน</u>

■ **<u>ผู้รับผิดชอบ</u>** ผู้จัดการแผนกเจ้าของข้อมูล

■ **<u>วิธีการปฏิบัติงาน</u>**

1) กำหนดมาตรฐานการเข้ามาใช้งาน

1.1) บริษัทฯ ต้องกำหนดสิทธิ์การเข้าใช้งานของผู้ใช้งานเพื่อยืนยันตัวตนของผู้ใช้งาน ก่อนเข้าสู่ระบบคอมพิวเตอร์แยกเป็นรายบุคคล (User name)

1.2) พนักงานต้องเก็บและรักษารหัสผ่าน (Password) สำหรับทุกระบบงานที่ได้รับมอบ เป็นความลับ

1.3) พนักงานต้องใช้ User Login และ Password ส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่ครอบครองอยู่หรือไปใช้เครื่องคอมพิวเตอร์ของผู้อื่นชั่วคราว โดย Password ส่วนบุคคลดังกล่าว ดังนี้

- Password จะต้องมีความยาวอย่างน้อย 8 ตัวอักษร และมีการผสมผสานระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน เช่น Praram#9
- ไม่กำหนด Password ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
- ไม่กำหนด Password ส่วนบุคคลจากคำศัพท์ที่ใช้ในพจนานุกรม
- กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก 90 วัน
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ เปลี่ยนรหัสผ่านนั้นโดยทันที

1.4) พนักงานต้องกำหนด Password สำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายของบริษัทฯ

1.5) พนักงานต้องไม่จดหรือบันทึก Password ส่วนบุคคลไว้ในสถานที่โล่งแจ้งที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

1.6) กรณีที่มีความจำเป็นที่จะต้องบอก Password แก่ผู้อื่นเนื่องจากความจำเป็นของงานหลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยน Password ทันที

2) กำหนดระเบียบในการ Login เข้าใช้งานในระบบคอมพิวเตอร์

2.1) การ Login เข้าใช้งาน Applications ของบริษัทฯ ผู้ใช้งานจะต้อง Login เข้าระบบด้วยตนเอง ห้ามไม่ให้ผู้อื่นดำเนินการให้

2.2) ไม่อนุญาตให้บุคคลอื่น ใช้งานบัญชีผู้ใช้ของตนเอง

2.3) ไม่อนุญาตให้นำบัญชีผู้ใช้ของตนเอง Login เข้าสู่ระบบ แล้วให้ผู้อื่นใช้งาน

2.4) ให้ Logout ระบบเมื่อใช้งานเสร็จแล้วหรือไม่ได้ใช้งานเป็นเวลานาน

4.3) <u>การควบคุมของระบบฐานข้อมูล</u>

■ **<u>ผู้รับผิดชอบ</u>** พนักงานส่วนสนับสนุนเทคโนโลยีสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) กำหนดมาตรฐานการติดตั้งระบบฐานข้อมูล

1.1) ผู้ติดตั้งระบบฐานข้อมูล จะต้องเป็นพนักงานในส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัทฯ ซึ่งบริษัทฯ ได้มอบหมายให้ทำหน้าที่ดังกล่าว ทั้งนี้จะต้องมีพนักงานในส่วนสนับสนุนสารสนเทศร่วมดำเนินการด้วย

1.2) ผู้ติดตั้งระบบฐานข้อมูลจะต้องใช้ซอฟท์แวร์ที่มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

1.3) ส่วนสนับสนุนสารสนเทศ หรือพนักงานของบริษัทฯ ที่ได้รับมอบหมาย ให้เป็นผู้ติดตั้ง Patch ของระบบฐานข้อมูล จะต้องคำนึงถึง

- ผลกระทบของการติดตั้งต่อผู้ใช้งานหรือระบบงานที่เกี่ยวข้อง
- ประเมินความเสี่ยงของการติดตั้ง Patch ดังกล่าว
- แจ้งให้ส่วนที่เกี่ยวข้องได้รับทราบกำหนดวันและเวลาการติดตั้งดังกล่าว
- เตรียมการเพื่อย้อนกลับมาสู่ระบบเดิมหากการติดตั้งไม่สำเร็จ รวมทั้ง รายงานผลการติดตั้ง ให้กับผู้บังคับบัญชาได้รับทราบ

2) กำหนดมาตรฐานของผู้ใช้งาน (User Identification) และการอนุมัติการใช้งาน (Authorization)

2.1) กำหนดมาตรฐานของผู้ใช้งาน ต้องมีการกำหนดกลุ่มใช้งาน ดังนี้

- OS Userได้แก่ Super User, Developer, Operation, DBA, Audit
- Database User ได้แก่ DB Super User (SQL Administrator) ,DB Owner Tables, DB Users ,Audit User
- Application User ได้แก่ Read Only Users, Update Users, Admin Users,Audit Users

หากมีความจำเป็นต้องเพิ่ม กลุ่มผู้ใช้งานใหม่ ต้องขออนุมัติอย่างเป็นลายลักษณ์อักษรกับผู้จัดการแผนกเทคโนโลยีสารสนเทศ

2.2) มาตรฐานการอนุมัติการใช้งาน (Authorization)

- เมื่อผู้ใช้งานได้รับความเห็นชอบจากหัวหน้างานและผู้จัดการแผนกต้นสังกัดตามลำดับขั้นตอนในการขอใช้งานระบบฐานข้อมู แผนกเทคโนโลยีสารสนเทศ ในส่วนผู้ดูแลระบบฐานข้อมูล ต้องจัดทำทะเบียนผู้ใช้งานให้สอดคล้องกับกลุ่มของผู้ใช้งานตามข้อ 2.1

3) กำหนดมาตรฐานในการเข้าใช้งาน (Login) และการเข้าถึงข้อมูล (Access Control) ในระบบฐานข้อมูล

3.1) กำหนดมาตรฐานการเข้ามาใช้งาน (Login)

- การตั้งชื่อ User Login จะต้องมีอย่างน้อย 8 ตัวอักษร
- มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- ไม่กำหนด Password ส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน
- ไม่กำหนด Password ส่วนบุคคลจากคำศัพท์ที่ใช้ในพจนานุกรม
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านโดยทันที

3.2) กำหนดมาตรฐานการเข้าถึงข้อมูล (Access Control)

- กำหนดวิธีการเข้าถึงข้อมูล ให้สอดคล้องกับกลุ่มของผู้ใช้งานระบบ
  - Super User = ALL
  - DBA User = Tables (Create/Drop/Read/write/Insert/delete),Grant Privilege
  - Operator User = Read (For Backup)
  - Audit User = Read
- กำหนดมาตรฐานการตั้งชื่อกลุ่มผู้ใช้งานระบบฐานข้อมูล (DB Roles) โดยให้ขึ้นต้นด้วยตัวย่อของระบบงานและให้มีความยาวไม่เกิน 3 ตัวอักษรและตามด้วยเครื่องหมาย '_' และชื่อกลุ่มผู้ใช้งานระบบ

4) กำหนดมาตรฐานในการส่งข้อมูลผ่านระบบเครือข่าย (Data Exchange) ส่วนสนับสนุนสารสนเทศจะเป็นผู้ Setup Permission ของ Patch ที่ใช้เก็บ Data ในการ Interface เพื่อใช้ในการแลกเปลี่ยนข้อมูลผ่านระบบเครือข่าย

5) กำหนดมาตรฐานของการตรวจสอบการเข้าใช้งาน (Audit Trail) และความถูกต้องของข้อมูล (Data Integrity) ในระบบฐานข้อมูล

5.1) ตรวจสอบการเข้าใช้ระบบฐานข้อมูล โดยผู้ใช้งานและรายงานสรุปให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

5.2) ตรวจสอบความถูกต้องของข้อมูล (Data Integrity) ร่วมกับสำนักควบคุมภายในและจัดทำรายงานผลการตรวจสอบให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

6) กำหนดมาตรฐานการสำรองข้อมูลและการนำกลับมาใช้ เพื่อป้องกันข้อมูลเสียหาย

6.1) ส่วนสนับสนุนสารสนเทศ ต้องพิจารณาจัดหา Media ที่มีประสิทธิภาพเพื่อใช้ในการสำรองข้อมูล

6.2) ส่วนสนับสนุนสารสนเทศและฝ่าย/ส่วนงานที่เกี่ยวข้องต้องร่วมกันพิจารณาถึงวิธีสำรองและติดตั้งข้อมูลของแต่ละระบบงาน

6.3) ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบการสำรองข้อมูลว่าทำสำเร็จหรือไม่ และหากไม่สำเร็จต้องดำเนินการแก้ไข

6.4) การ Restore Data สามารถกระทำได้เฉพาะผู้ที่ได้รับมอบหมาย หรือสั่งการจากผู้จัดการแผนกเทคโนโลยีสารสนเทศ

6.5) ส่วนสนับสนุนสารสนเทศ ต้องจัดเก็บ Media ที่ใช้ในการสำรองข้อมูลไว้ในสภาพแวดล้อมที่เหมาะสมและมีระบบรักษาความปลอดภัยที่ดี เพื่อเก็บรักษาไว้

6.6) ส่วนสนับสนุนสารสนเทศ ต้องตรวจสอบสภาพ Media และข้อมูลที่อยู่ใน Media อย่างสม่ำเสมอว่ายังอยู่ในสภาพที่ใช้งานได้ดีหรือไม่ หากพบปัญหาให้รีบดำเนินการแก้ไข

4.4) <u>การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)</u>

■ **<u>ผู้รับผิดชอบ</u>** พนักงานส่วนสนับสนุนสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) การติดตั้งเครื่องคอมพิวเตอร์ Server ต่างๆ ต้องมีการจัดทำแบบแปลนการติดตั้งอุปกรณ์บนตู้ Rack แสดงตำแหน่งต่าง ๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทฯ ระบุไว้ โดยจัดเก็บไว้ในส่วนสนับสนุนสารสนเทศ
2) การติดตั้งอุปกรณ์สื่อสารข้อมูล และอุปกรณ์รักษาความปลอดภัยต่าง ๆ ต้องมีการจัดทำแบบแปลนการติดตั้งบนตู้ Rack แสดงตำแหน่งต่างๆ ของอุปกรณ์บนตู้ Rack ในรูปแบบที่บริษัทฯระบุไว้ โดยจัดเก็บไว้ที่ส่วนสนับสนุนสารสนเทศ
3) การติดตั้งอุปกรณ์สื่อสารข้อมูลทุกชนิดกับระบบงานต่าง ๆ ของบริษัทให้อยู่ในความควบคุมดูแลของส่วนงานสนับสนุนสารสนเทศ
4) การติดตั้งอุปกรณ์ดับเพลิง ระบบเครื่องปรับอากาศ และระบบเครื่องจ่ายไฟสำรองฉุกเฉิน จะต้องมีมาตรฐานตามที่บริษัทฯ หรือผู้ผลิตกำหนดไว้

4.5) <u>การรักษาความปลอดภัยระบบคอมพิวเตอรเครือข่าย</u>

■ **<u>ผู้รับผิดชอบ</u>** พนักงานส่วนสนับสนุนสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) กำหนดมาตรฐานในการติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัทฯ ผ่านทางเครือข่าย

ทำการติดตั้ง Service Pack ตลอดจน Patch ต่าง ๆ ให้ทันสมัยรวมทั้ง Software Antivirus ตามที่บริษัทฯ กำหนด

2) กำหนดมาตรฐานของระบบรักษาความปลอดภัยบนระบบเครือข่าย

2.1) กำหนดให้มีอุปกรณ์ Firewall สำหรับเครือข่ายของบริษัทฯ ภายในกับเครือข่ายภายนอก

2.2) ทำการอัพเดต firmware ของ firewall เพื่อให้ทันสมัยต่อความเปลี่ยนแปลงของภัยคุกคามทางด้านเครือข่าย

2.3) จัดเก็บทะเบียนเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ที่มีการควบคุมการใช้งาน

2.4) จัดทำและปรับปรุง Configuration ของระบบเครือข่ายให้มีความทันสมัยและปลอดภัยอยู่เสมอ

2.5) ทำการ Backup Configuration ของอุปกรณ์สื่อสารข้อมูล อย่างน้อยครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง

2.6) จัดการเปลี่ยน Password ของอุปกรณ์สื่อสารของบริษัทฯ ทุกชุด อย่างน้อยปีละ 1 และให้พิมพ์ ครั้ง 1 รายละเอียดของอุปกรณ์ Password ใส่ซองปิดผนึกและให้หัวหน้าส่วนสนับสนุนสารสนเทศ ลงชื่อกำกับและส่งต่อให้ผู้จัดการแผนกเทคโนโลยีสารสนเทศ

2.7) ห้ามใช้ Community Name ของอุปกรณ์สื่อสารข้อมูลทุกชนิด หรืออุปกรณ์อื่นที่ใช้ Protocol SNMP ที่ถูกกำหนดชื่อ มาโดยผู้ผลิตอุปกรณ์ เมื่อเริ่มใช้งานกับระบบงานของบริษัทฯ ให้ดำเนินการเปลี่ยนชื่อนั้นโดยทันที

2.8) สำหรับ Server ที่จะทำการติดตั้งเข้ากับเครือข่ายของบริษัทฯ โดยพนักงานบริษัทฯ หรือบริษัทผู้ดูแลการติดตั้ง Server ดังกล่าว ต้องส่งรายละเอียดของระบบปฏิบัติการ (Operating System) และ Service Pack หรืออื่น ๆ ที่จำเป็นสำหรับการติดตั้งให้กับแผนกเทคโนโลยีสารสนเทศ ในส่วนสนับสนุนสารสนเทศรับทราบข้อมูลก่อน หลังจากนั้นจึงจะจ่าย IP Address ให้และทำการ Monitor Port ที่จ่ายให้กับ Server ดังกล่าวไม่น้อยกว่า 1 สัปดาห์อย่างใกล้ชิด

2.9) ให้ส่วนสนับสนุนสารสนเทศ เป็นผู้ถือกุญแจห้องอุปกรณ์สื่อสาร/ห้อง Server ของบริษัทฯ

3) กำหนดให้มีการจัดทำแผนผังเครือข่ายของบริษัทฯ

ให้มีการจัดทำแผนผังเครือข่ายของบริษัทฯ และต้องปรับปรุงแผนผังดังกล่าวให้มีความทันสมัยอยู่เสมอ รวมทั้งจัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

4.6) การป้องกันไวรัสคอมพิวเตอร์/มัลแวร์

■ **ผู้รับผิดชอบ** เจ้าหน้าที่ส่วนสนับสนุนสารสนเทศ / เจ้าหน้าที่ส่วนพัฒนาระบบสารสนเทศ

■ **วิธีการปฏิบัติงาน**

1) ติดตั้งและตรวจสอบเครื่องมือในการกำจัดไวรัสคอมพิวเตอร์/มัลแวร์

1.1) ติดตั้งและตรวจสอบ ระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์สำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Server Protect and Office Scan) เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้ง ต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้นๆ ทุก 24 ชั่วโมง

1.2) ติดตั้งและตรวจสอบระบบป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ให้กับเครื่องลูกข่ายของบริษัทฯทุกเครื่อง เพื่อให้มีการทำงานอย่างต่อเนื่องและถูกต้อง รวมทั้งต้องจัดให้มีการอัพเดตจากเจ้าของผลิตภัณฑ์นั้น ๆ ทุก 24 ชั่วโมง

2) กำหนดหน้าที่และความรับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์

2.1) กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์บนเครื่องคอมพิวเตอร์ส่วนบุคคล ไม่ให้แพร่กระจายทำความเสียหายกับข้อมูลของบริษัทฯ

2.2) กำหนดให้ส่วนบริการผู้ใช้เทคโนโลยีสารสนเทศ ต้องมีการแจ้งข่าวเกี่ยวกับไวรัสคอมพิวเตอร์/มัลแวร์ทันทีหากมีการระบาดของไวรัสคอมพิวเตอร์/มัลแวร์ตัวใหม่

2.3) กำหนดให้ส่วนเทคนิคปฏิบัติการเครือข่าย มีหน้าที่รับผิดชอบในการตรวจจับและทำลายไวรัสคอมพิวเตอร์/มัลแวร์อย่างสม่ำเสมอบน Server และอุปกรณ์เครือข่าย เพื่อป้องกันความเสียหายกับข้อมูลของบริษัทฯ

2.4) กำหนดให้ส่วนเทคนิคปฏิบัติการเครือข่าย ทำการรายงานสถิติการติดไวรัสคอมพิวเตอร์/มัลแวร์ของเครื่องคอมพิวเตอร์ส่วนบุคคลที่แสดงอยู่บนเซิร์ฟเวอร์แม่ข่ายสำหรับป้องกันไวรัสคอมพิวเตอร์/มัลแวร์ของบริษัท

5) **การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)**

เพื่อสร้างความมั่นใจว่าการซื้อหรือการพัฒนามีความสอดคล้องกับแผนงานของบริษัทฯ มีหลักเกณฑ์ในการคัดเลือก พัฒนาและมีการจัดลำดับความสำคัญของงาน รวมทั้งกระบวนการพัฒนาได้มีการทดสอบอย่างเพียงพอว่าระบบงานที่แก้ไขเปลี่ยนแปลงมีความถูกต้องและให้ผลลัพธ์ตามที่ได้กำหนดไว้

■ **วัตถุประสงค์** เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้านแก้ไขเปลี่ยนแปลง (Integrity Risk)

■ **ผู้รับผิดชอบ** เจ้าหน้าที่ส่วนสนับสนุนสารสนเทศ / เจ้าหน้าที่ส่วนพัฒนาระบบสารสนเทศ / ผู้บริหารหน่วยงานที่ต้องการพัฒนาหรือแก้ไขแปลี่ยนแปลงวิธีการทำงานนั้น

■ **วิธีการปฏิบัติงาน**

1) กำหนดให้ปฏิบัติตามขั้นตอนในการพัฒนาซอฟต์แวร์ ดังนี้

- การเริ่มต้นโครงการ (Initiation) ได้รับคำสั่งให้มีการพัฒนาหรือแก้ไขระบบ มอบหมายงานแบ่งแยกหน้าที่
- การวิเคราะห์ระบบ (Analysis) โดยต้องคำนึงถึง “การเปลี่ยนแปลง (Change)” ที่มีส่วนสำคัญและกระทบกับการทำงานเดิม ต้องประเมิน Risk of Change ตามวิธีปฏิบัติการบริหารการเปลี่ยนแปลงด้วย
- การออกแบบระบบ (Design)
- การพัฒนาและทดสอบระบบ (Build and Test)

- การติดตั้งและใช้งานระบบ (Deployment)

2) กำหนดให้จัดทำเอกสารสิ่งที่ต้องส่งมอบขั้นต่ำตามที่แสดงไว้ในตาราง

ลำดับ	ขั้นตอน	สิ่งที่ส่งมอบ
1	การเริ่มต้นโครงการ (Initiation)	- ปัญหา - เหตุผลความจำเป็น - ความต้องการของผู้ใช้งานระบบ (User requirement)
2	การวิเคราะห์ระบบ (Analysis)	- เอกสาร System flow diagram - เอกสาร data flow diagram level 1-2 - รายการประเมินการจัดการการเปลี่ยนแปลง (Manage of Change Checklist)
3	การออกแบบ (Design)	- เอกสาร program specification - เอกสาร test case ที่ใช้ในการทดสอบ
4	การพัฒนาและทดสอบ (Build and Test)	- คู่มือการใช้งานสำหรับผู้ใช้งาน - คู่มือการใช้งานสำหรับผู้ดูแลระบบ - Source code ของระบบ - เอกสารผลการทดสอบตาม Test case
5	การติดตั้งและใช้งาน (Deployment)	- Source code ที่เป็นเวอร์ชั่น ที่จะนำขึ้นสู่ Production ต้องนำไปเก็บไว้กับผู้ที่ได้รับมอบหมายให้ดูแลรักษา

6) **การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)**

บริษัทฯ ต้องกำหนดวิธีปฏิบัติกรณีเกิดเหตุการณ์ฉุกเฉินในกรณีต่างๆ และกำหนดหน้าที่รับผิดชอบของแต่ละบุคคล พร้อมทั้งมีการซักซ้อมเป็นระยะ เพื่อให้เกิดผลกระทบต่อการบริการของบริษัทฯ แก่ลูกค้าให้น้อยที่สุดและยังสามารถดำเนินงานต่อไปได้โดยไม่ติดขัด

- **<u>วัตถุประสงค์</u>** เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน
- **<u>ผู้รับผิดชอบ</u>** เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ
- **<u>วิธีการปฏิบัติงาน</u>**

1) กำหนดหน้าที่ความรับผิดชอบ

1.1) ติดตั้งอุปกรณ์ Hardware ติดตั้งโปรแกรม OS และทดสอบการใช้งานให้มีความพร้อมในกรณีที่เหตุการณ์ฉุกเฉินโดยส่วนสนับสนุนสารสนเทศและส่วนพัฒนาระบบสารสนเทศ

1.2) ติดตั้งอุปกรณ์เครือข่ายให้สามารถใช้งานได้ โดยส่วนที่ดูแลเครือข่ายคอมพิวเตอร์

1.3) จัดหาอุปกรณ์อำนวยความสะดวก (Facility) ให้มีความพร้อมในการใช้งานโดยส่วนสนับสนุนสารสนเทศ

1.4) นำข้อมูลสำรองชุดล่าสุดมาลงในระบบเพื่อใช้งาน โดยส่วนสนับสนุนสารสนเทศ

1.5) ทดสอบการใช้งานเพื่อเตรียมความพร้อมอย่างสม่ำเสมอ โดยส่วนสนับสนุนสารสนเทศและพัฒนาระบบสารสนเทศ

1.6) กำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน

1.7) พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องเข้ารับการอบรมหรือสร้างความตระหนักเพื่อให้รู้หรือทราบวิธีปฏิบัติในกรณีที่เกิดเหตุฉุกเฉิน ในกรณีต่าง ๆ

2) กำหนดมาตรฐานสำหรับห้องเซิร์ฟเวอร์ (Server) สำรอง

2.1) ติดตั้งและดูแลระบบคอมพิวเตอร์สำรองอย่างสม่ำเสมอเพื่อให้สามารถให้บริการทดแทนระบบคอมพิวเตอร์หลักได้

2.2) ติดตั้งข้อมูลระบบ Facility ให้พร้อมสำหรับการใช้งานอย่างสม่ำเสมอ

2.3) นำข้อมูลที่สำรองไว้มา Update ให้มีความทันสมัยอยู่ตลอดเวลา

2.4) ทดสอบการใช้งานระบบคอมพิวเตอร์ เครือข่ายและระบบ Facility อย่างสม่ำเสมอ เพื่อให้สามารถใช้งานได้โดยไม่ติดขัด

3) การสำรองข้อมูล

3.1) ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System Softwares) โปรแกรมระบบงานคอมพิวเตอร์ (Application Softwares) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

3.2) จัดทำขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียดดังนี้

- ข้อมูลที่ต้องสำรองและความถี่ในการสำรอง
- ประเภทสื่อบันทึก (Media)
- จำนวนที่ต้องสำรอง (Copy)
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

3.3) จัดทำบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3.4) ทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้

3.5) จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีการปฏิบัติงานต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องมีการควบคุมการเข้าออกและระบบป้องกันความเสียหายที่เป็นมาตรฐาน

3.6) ต้องจัดทำฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อสำรองข้อมูล เพื่อให้สามารถค้นหาได้โดยเร็ว

3.7) การขอใช้งานสื่อบันทึกข้อมูลสำรอง ควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียด เกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล วันที่และเวลา

7) **การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation)**

บริษัทฯ ต้องกำหนดวิธีการปฏิบัติงานประจำด้านคอมพิวเตอร์ไว้เป็นลายลักษณ์อักษร เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่และควรมีการจัดทำบันทึกผลการปฏิบัติงานไว้เพื่อให้สามารถตรวจสอบได้ว่ามีการปฏิบัติงานครบถ้วนและเป็นไปตามวิธีการปฏิบัติงานที่กำหนดไว้

- **<u>วัตถุประสงค์</u>** เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่องและมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆ ซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหาและการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk และ Availability Risk
- **<u>ผู้รับผิดชอบ</u>** เจ้าหน้าที่ส่วนสนับสนุนสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) จัดทำขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (computer operator) และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
2) กำหนดมาตรฐานการ Login เข้าใช้งานระบบ โดยต้องบันทึกข้อมูลที่เกี่ยวข้องกับการ Login นั้นไว้ และให้บันทึกทั้งการ Login ที่ทำได้สำเร็จและไม่สำเร็จ เพื่อใช้ในการตรวจสอบภายหลัง
3) ควรกำหนดให้มีการบันทึก (log book) รายละเอียดเกี่ยวกับการปฏิบัติงานประจำในด้านต่าง ๆ โดยบันทึกดังกล่าวควรมีรายละเอียดในเรื่องต่อไปนี้
   - ผู้ปฏิบัติงาน
   - เวลาปฏิบัติงาน
   - รายละเอียดการปฏิบัติงาน
   - ปัญหาที่เกิดขึ้นและการแก้ไข

   การปฏิบัติงานประจำ ควรประกอบด้วย
   - การสำรองข้อมูล
   - การตรวจสอบความพร้อมของอุปกรณ์คอมพิวเตอร์ในห้องเซิร์ฟเวอร์ (Server Room)
   - การตรวจสอบซอฟท์แวร์ระบบ ระบบเครือข่ายและระบบป้องกันไวรัส
   - การตรวจสอบความพร้อมของอุปกรณ์ป้องกันภัยหรืออุปกรณ์อื่น ที่เกี่ยวข้อง เช่น ระบบดับเพลิง ระบบควบคุมอุณหภูมิ
   - การตรวจสอบและบำรุงรักษาอุปกรณ์

8) **การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)**

การกำหนดนโยบาย ระเบียบปฏิบัติ มาตรฐานและแนวทางในการคัดเลือกผู้ให้บริการภายนอก จะช่วยให้การตัดสินใจมีประสิทธิผลที่ดีขึ้น ซึ่งส่งผลต่อค่าใช้จ่ายที่เหมาะสมในการเลือกใช้บริการและผลของการให้บริการเป็นไปตามที่คาดหวังไว้

■ **<u>วัตถุประสงค์</u>** เพื่อให้บริษัทฯ ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น ได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือและสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

■ **<u>ผู้รับผิดชอบ</u>** ผู้บริหารระดับสูง / ผู้จัดการแผนกเทคโนโลยีสารสนเทศ / เจ้าหน้าที่ส่วนพัฒนาระบบสารสนเทศ

■ **<u>วิธีการปฏิบัติงาน</u>**

1) การคัดเลือกผู้ให้บริการจากภายนอก การคัดเลือกผู้ให้บริการจากภายนอกให้เป็นไปตามระเบียบวิธีการคัดเลือกตามกระบวนการจัดซื้อจัดจ้าง โดยการพิจารณาคัดเลือกต้องครอบคลุมเรื่องดังต่อไปนี้

1.1) การเปรียบเทียบข้อเสนอกับความต้องการของบริษัทฯ

1.2) การประเมินผลงานที่ผ่านมาของผู้ให้บริการภายนอก

1.3) กำหนดมาตรฐานของอุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องเป็นอุปกรณ์ที่มีคุณภาพและได้มาตรฐาน
   - อุปกรณ์ที่นำมาติดตั้งต้องมีมาตรฐานรับรองจากบริษัทฯ หรือจากผู้ผลิตโดยตรง
   - อุปกรณ์ที่นำมาติดตั้งใช้งานจะต้องมีมาตรฐานที่เป็นสากล (Standard)

2) การควบคุมด้านความมั่นคงปลอดภัย

2.1) กำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ที่บริษัทฯ ทำสัญญาว่าจ้างให้มาปฏิบัติงานซึ่งสอดคล้องกับนโยบายความมั่นคงปลอดภัยฯ ของบริษัทฯ และให้ผู้ปฏิบัติงานนั้น ลงนามในเอกสารดังกล่าว

2.2) เมื่อสิ้นสุดการจ้างงานหรือการเปลี่ยนแปลงลักษณะการจ้างงานของหน่วยงานภายนอกจะต้องถอนสิทธิ์การเข้าถึงระบบสารสนเทศและทรัพย์สินสารสนเทศทันที

3) การควบคุมระหว่างการให้บริการ

3.1) ต้องควบคุมผู้ให้บริการจากภายนอกว่ามีการปฏิบัติตามข้อกำหนดที่จัดทำขึ้นอย่างสม่ำเสมอ เช่น ดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ

3.2) ต้องมีการกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือการให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การปรับปรุงเทคโนโลยี ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

4.4 <u>สิทธิและทรัพย์สินของบริษัทฯ</u>

สิ่งประดิษฐ์ใดๆ ที่พนักงานค้นคิดหรือร่วมกันคิดค้นระหว่างที่พนักงานทำงานกับบริษัทฯ ถือว่าเป็น สิทธิและทรัพย์สินของบริษัทฯ พนักงานจะนำไปเปิดเผยหรือใช้เป็นผลประโยชน์ไม่ได้ ได้แก่

4.4.1 ข้อมูลหมายรวมถึงข้อมูลที่เป็นอิเล็กทรอนิกส์และข้อมูลที่เป็นเอกสาร สิ่งพิมพ์ ข้อมูลภาพ/เสียง เป็นต้น

4.4.2 ระบบงานครอบคลุมถึงระบบข้อมูลและการใช้ระบบคอมพิวเตอร์

4.4.3 คอมพิวเตอร์ครอบคลุมถึงระบบคอมพิวเตอร์ ระบบการสื่อสารและอุปกรณ์การคำนวณที่เกี่ยวข้อง

4.5 <u>การพิจารณาโทษทางวินัยและการเรียกค่าเสียหาย</u>

4.5.1 พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ โดยจงใจหรือประมาณเลินเล่อและก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใด บริษัทฯจ ะพิจารณาดำเนินการทางวินัยและความรับผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมายข้อบังคับ ระเบียบหรือประกาศที่เกี่ยวข้อง ผู้บังคับบัญชาผู้ใด งดเว้นหรือละเว้น การปฏิบัติตามหน้าที่และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายความมั่นคงปลอดภัยระบบสารสนเทศนี้ ให้นำบทบัญญัติในวรรคก่อนมาใช้บังคับโดยอนุโลม

4.5.2 การฝ่าฝืนข้อกำหนดใด ๆ ตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศนี้ แม้จะไม่ก่อให้เกิดความเสียหายแก่บริษัทฯ หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือนหรือเลื่อนตำแหน่งด้วยก็ได้

นโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2568 วันที่ 7 พฤศจิกายน 2568 โดยมีผลบังคับใช้ตั้งแต่วันที่ 10 พฤศจิกายน 2568 เป็นต้นไป

(นายภวัต วงศ์ตั้งตระกูล)
ประธานกรรมการบริษัท