ประกาศที่ IT.001/2565
เรื่อง : นโยบายระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Policy)

วัตถุประสงค์ (Objective)

1.1 เพื่อรักษาซึ่งความมั่นคงปลอดภัยของข้อมูลอันประกอบไปด้วย การรักษาความลับของข้อมูล (Confidential) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

1.2 เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง เช่น พนักงาน และ ผู้ให้บริการภายนอก

บทนำ

นโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ ของบริษัทฯ จัดตั้งขึ้นตามข้อกำหนดของมาตรฐาน TISAX (Trusted Information Security Assessment Exchange) เพื่อให้มีการกำหนดทิศทางการบริหารจัดการ และการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศ โดยสอดคล้องกับความต้องการทางธุรกิจ และกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องโดยมีการกำหนดนโยบายในแต่ละด้าน เผยแพร่ และบังคับใช้กับพนักงาน ผู้ให้บริการภายนอกที่มีการเข้าถึงข้อมูลที่ใช้ภายในของบริษัทฯ ซึ่งจะมีการแบ่งนโยบายบริหารความมั่นคงปลอดภัยสารสนเทศ เป็นหมวดหมู่ ดังต่อไปนี้

นโยบายการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (Project Management Policy)

พนักงาน ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ เพื่อให้มีการควบคุม ข้อมูลที่เป็นความลับของลูกค้า และของบริษัทฯ ในการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศได้อย่างมั่นคงปลอดภัย ตั้งแต่ก่อนเริ่มจัดตั้งโครงการจนกระทั่งถึงโครงการเสร็จสิ้น ซึ่งขอบข่ายโครงการด้านเทคโนโลยีสารสนเทศ เช่น การปรับปรุงระบบสารสนเทศ การนำระบบฐานข้อมูลหรือ ERP มาใช้งาน การปรับปรุงระบบเครือข่ายภายในกลุ่มบริษัทฯ ตลอดจนโครงการที่เกี่ยวข้องกับการพัฒนาผลิตภัณฑ์ใหม่ (Advance Product Quality Planning: APQP)

นโยบายความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล เพื่อให้พนักงาน และผู้ให้บริการภายนอกเข้าใจในหน้าที่ความรับผิดชอบของตนเอง และมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา ตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง และเพื่อป้องกันผลประโยชน์ของบริษัทฯ

นโยบายการบริหารจัดการทรัพย์สิน (Asset Management Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายการบริหารจัดการทรัพย์สิน เพื่อให้มีการระบุทรัพย์สินของบริษัทฯ และกำหนดหน้าที่ความรับผิดชอบในการดูแลทรัพย์สินตามระดับการป้องกันที่เหมาะสม และป้องกันการเปิดเผยข้อมูลของบริษัทฯ โดยไม่ได้รับอนุญาต ทั้งนี้รวมถึงการเปลี่ยนแปลงจัดการข้อมูลที่อยู่ในทรัพย์สิน การขนย้าย การลบ หรือการทำลายข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูล

นโยบายการควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศ (Access Control Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายการควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูลสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบสารสนเทศและบริการโดยไม่ได้รับอนุญาต และเพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน และจะไม่มีการเข้าใช้งาน Website ภายนอกกรณีที่ไม่เกี่ยวข้องกับการปฏิบัติงาน และไม่ทำผิด พรบ.คอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้อง

นโยบายการเข้ารหัสข้อมูล (Cryptography Control Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยของบริษัทฯ ต้องปฏิบัติตามนโยบายการเข้ารหัสข้อมูล เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม และป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ ซึ่งจะไม่มีการเขียนรหัสผ่านไว้ เพื่อป้องกันรหัสผ่านมีการเปิดเผยไปสู่บุคคลอื่นที่ไม่ได้รับอนุญาตในการเข้าถึงข้อมูล หากมีสิ่งที่น่าสงสัยให้ดำเนินการเปลี่ยนรหัสผ่านโดยทันที และไม่ใช้รหัสผ่านอันเดียวกันสำหรับการเข้าระบบที่ไม่เกี่ยวข้องกับการปฏิบัติงาน และเมื่อมีการเข้าระบบงานในครั้งแรกแล้วจะต้องดำเนินการเปลี่ยนรหัสผ่านใหม่ทันที เพื่อป้องกันข้อมูลของรหัสผ่านไม่ให้รั่วไหลสู่บุคคลอื่น การตั้งค่ารหัสผ่านจะต้องมีอย่างน้อย 8 ตัวอักษรขึ้นไป พร้อมมีตัวอักษรพิเศษเพื่อทำให้เกิดการคาดเดาได้ยากขึ้น

นโยบายความปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายความปลอดภัยทางกายภาพและสภาพแวดล้อม เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต โดยมีการกำหนดพื้นที่ที่จะต้องมีการควบคุมข้อมูลที่มีความลับ และป้องกันความเสียหายจากการรั่วไหลของข้อมูล และการแทรกแซงการทำงานที่มีผลต่อข้อมูลสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศ รวมทั้งป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัทฯ

นโยบายความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับการดำเนินงาน เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศ และระบบงานสารสนเทศของบริษัทฯ เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย ได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี ได้รับการป้องกันจากการสูญหายของข้อมูล เพื่อให้ระบบงานสารสนเทศมีการบันทึกเหตุการณ์และจัดทำหลักฐาน มีการทำงานที่ถูกต้องและมีการป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค และเพื่อลดผลกระทบของความไม่พร้อมในระบบให้บริการ

นโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เพื่อให้มีการป้องกันข้อมูลสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ และเพื่อให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการถ่ายโอนภายในบริษัทฯ หรือถ่ายโอนกับหน่วยงานภายนอก

นโยบายการจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบาย การจัดหา การพัฒนา และการบำรุงรักษาระบบ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ (System Development Life Cycle : SDLC) ซึ่งจะมีการกำหนดแนวทางการพัฒนา หรือ ใช้บริการระบบที่ถูกพัฒนาขึ้น ให้เป็นไปในทิศทางเดียวกัน และกำหนดขั้นตอนที่เพื่อให้ระบบให้มีข้อบกพร่องน้อยที่สุด เพราะงานการวิเคราะห์และพัฒนาระบบสารสนเทศดำเนินงานตามมาตรฐานในการพัฒนาระบบงาน และมีการทดสอบก่อนที่จะให้ผู้ใช้งานนำไปใช้ปฏิบัติงานจริง

นโยบายความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อให้มีการป้องกันทรัพย์สินและข้อมูลของบริษัทฯ ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก และเพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย ตลอดจนระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ (Service Level Agreement)

นโยบายการบริหารจัดการเหตุการณ์ผิดปกติในระบบความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายการบริหารจัดการเหตุการณ์ผิดปกติในระบบความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีวิธีการที่สอดคล้องกันในการรายงานเหตุผิดปกติ การแก้ไขปัญหาอย่างมีประสิทธิผล ซึ่งรวมถึงการแจ้งสถานการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศให้ผู้ที่เกี่ยวข้องได้รับทราบ

นโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ เพื่อให้ระบบสารสนเทศของบริษัทฯ ได้ถูกเตรียมความพร้อมกรณีที่มีเหตุการณ์ผิดปกติ หรือ ภัยพิบัติ รวมถึงการปฏิบัติดังกล่าวจะต้องทำให้มีความสอดคล้อง (Compliance) กับข้อกำหนดกฎหมาย และข้อกำหนดของลูกค้าที่เกี่ยวข้อง (Legal and other requirements) และสัญญาที่มีการลงนาม (Contract Agreement) เพื่อป้องกันการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้อง จึงต้องมีแนวทางการปฏิบัติ และขั้นตอนที่ชัดเจน รวมถึงทีมงานที่เกี่ยวข้อง

นโยบายสำหรับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ (End User Oriented Policy)

พนักงาน ผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ต้องปฏิบัติตามนโยบายสำหรับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มีกฎเกณฑ์การใช้งานสารสนเทศ ดูแลและควบคุมทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ อุปกรณ์ประมวลผลต่างๆอย่างเหมาะสม มีการป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญของบริษัทฯ มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่มีการถ่ายโอนภายใน หรือถ่ายโอนกับหน่วยงานภายนอก มีกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน และเพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา เป็นต้น

นโยบายการทบทวน และการปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Review and Improvement Policy)

นโยบายบริหารความมั่นคงปลอดภัยสารสนเทศฉบับนี้จะมีการทบทวน ในกรณีที่บริษัทฯ มีการปรับเปลี่ยนโครงสร้างการบริหารงาน หรือ เปลี่ยนแปลงผู้บริหารสูงสุด (ภายใน 45 วัน หลังจากการเปลี่ยนแปลง) ซึ่งหากที่ไม่มีการเปลี่ยนแปลงดังกล่าว นโยบายฉบับนี้จะต้องมีการทบทวนทุกปี โดยผู้บริหารสูงสุดร่วมกับคณะทำงาน (TISAX Committee) ในการประชุมทบทวนฝ่ายบริหาร ซึ่งจะมีวาระการประชุมที่ประกอบไปด้วย การทบทวนนโยบาย และKPI ที่ได้มีการติดตาม ตลอดจนแนวทางการปรับปรุงเป้าหมาย KPI อย่างต่อเนื่อง, การทบทวนทรัพย์สิน Asset Control list, การทบทวนความเสี่ยง, มาตรการควบคุมและการจัดทำ Risk Treatment Plan, ความเปลี่ยนแปลงต่างๆ ที่เกิดขึ้น และประสิทธิผลในการควบคุม, ผลการประเมินความสอดคล้องตามมาตรฐาน TISAX และความสอดคล้องตามกฎหมาย, รายงานความผิดปกติที่เกิดขึ้น และความไม่สอดคล้องที่เกิดขึ้น, สรุปผลการทบทวนเอกสารวิธีปฏิบัติในระบบ TISAX ตลอดจนแบบฟอร์มต่างๆ, ผลจากการประเมิน โดย Certify Body และการติดตามการปรับปรุงแก้ไขอย่างต่อเนื่อง, ข้อเสนอแนะเพื่อการปรับปรุง และผลการทบทวน การตัดสินใจจากฝ่ายบริหารและทรัพยากรที่จำเป็น

การลงโทษทางวินัย

ในกรณีกระทำการฝ่าฝืนนโยบายระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศนั้น มีความผิดชัดเจนและรุนแรง แม้จะเป็นการพบเพียงครั้งที่ 1 ก็ตาม ผู้บังคับบัญชาระดับสูงและฝ่ายทรัพยากรบุคคล จะต้องพิจารณาลงโทษทางวินัย ซึ่งอาจรวมไปถึงการถูกดำเนินคดีตามกฎหมายได้ ซึ่งมีโทษทั้งจำทั้งปรับ

ข้อยกเว้น

หากพนักงาน หรือผู้ให้บริการภายนอก ที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ไม่สามารถปฏิบัติตามนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือนโยบายแต่ละหมวดที่อ้างถึงได้ให้ชี้แจงเหตุผล และทำหนังสือขออนุญาตให้ผู้มีอำนาจอนุมัติเป็นกรณีไป ซึ่งข้อยกเว้นนั้นต้องมีระบบรักษาความปลอดภัยที่เหมาะสมมาทดแทน

จึงประกาศมาเพื่อทราบ และถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 1 กรกฎาคม 2565

.....

(นายพูลลาภ จิตราสวัสดิ์)
ผู้ช่วยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

.....

(นายอรรถสิทธิ์ องค์โฆษิต)
ผู้อำนวยการอาวุโสฝ่ายเทคโนโลยีสารสนเทศ

.....

(นายพิธาน องค์โฆษิต)
ประธานเจ้าหน้าที่บริหาร และ กรรมการผู้จัดการ