กฎบัตรของคณะกรรมการบริหารความเสี่ยง

บริษัท สโตนเฮ้นจ์ อินเตอร์ จำกัด (มหาชน)

กฎบัตรของคณะกรรมการบริหารความเสี่ยง

1. องค์ประกอบและคุณสมบัติของคณะกรรมการบริหารความเสี่ยง

1.1 คณะกรรมการบริหารความเสี่ยงจะต้องได้รับการแต่งตั้งจากคณะกรรมการบริษัท ประกอบด้วยคณะกรรมการบริษัท และ/หรือผู้บริหารของบริษัทอย่างน้อยจำนวน 3 ท่าน โดยที่คณะกรรมการบริษัทจะแต่งตั้งกรรมการบริหารความเสี่ยงคนหนึ่งเป็นประธานกรรมการบริหารความเสี่ยง

1.2 เป็นผู้มีความเข้าใจในธุรกิจ และมีประสบการณ์ตรงในธุรกิจ เพื่อกำหนดนโยบายด้านการบริหารความเสี่ยงให้ครอบคลุมทั้งองค์กร รวมทั้งกำกับดูแลให้มีระบบหรือกระบวนการบริหารจัดการความเสี่ยง เพื่อลดผลกระทบต่อธุรกิจของบริษัทฯ อย่างเหมาะสม

1.3 กำหนดให้คณะกรรมการบริหารความเสี่ยงต้องแต่งตั้งเลขานุการคณะกรรมการบริหารความเสี่ยง โดยอาจเป็นหัวหน้าสายงานสนับสนุนธุรกิจ หรือบุคคลที่คณะกรรมการบริหารความเสี่ยงเห็นสมควร ซึ่งบุคคลดังกล่าวต้องสนับสนุนและคอยช่วยเหลือการทำหน้าที่ของคณะกรรมการบริหารความเสี่ยง ตลอดจนการจัดเตรียมวาระการประชุม และบันทึกรายงานการประชุมของคณะกรรมการบริหารความเสี่ยง

2. หน้าที่และความรับผิดชอบของคณะกรรมการบริหารความเสี่ยง

2.1 กำหนด และทบทวน นโยบาย กรอบการบริหารความเสี่ยงองค์กร

2.2 กำกับดูแลและสนับสนุนให้มีการดำเนินงานด้านการบริหารความเสี่ยงองค์กร ให้สอดคล้องกับกลยุทธ์และเป้าหมายทางธุรกิจ รวมถึงสภาวการณ์ที่เปลี่ยนแปลงไป

2.3 พิจารณารายงานผลการบริหารความเสี่ยงองค์กร และให้ข้อคิดเห็นในความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้ง แนวทางการกำหนดมาตรการควบคุม หรือบรรเทา และการพัฒนาระบบการจัดการบริหารความเสี่ยงองค์กรให้มีประสิทธิภาพอย่างต่อเนื่อง

2.4 รายงานผลการบริหารความเสี่ยงองค์กรให้คณะกรรมการตรวจสอบ และคณะกรรมการบริษัทรับทราบ และในกรณีที่มีปัจจัย หรือเหตุการณ์สำคัญ ซึ่งอาจมีผลกระทบต่อบริษัท อย่างมีนัยสำคัญ ต้องรายงานต่อคณะกรรมการบริษัทเพื่อทราบและพิจารณาโดยเร็วที่สุด

2.5 วางกรอบการดำเนินงานและควบคุมดูแลการบริหารความเสี่ยงทั่วทั้งองค์กร ภายใต้การนำของประธานเจ้าหน้าที่บริหาร โดยกรณีผู้บริหารพบว่านโยบายการบริหารความเสี่ยงทั่วทั้งองค์กรไม่เหมาะสมกับสภาพการดำเนินงาน ต้องมีการนำเสนอคณะกรรมการของบริษัท ผ่านคณะกรรมการบริหารความเสี่ยงเพื่อขออนุมัติในการปรับปรุงนโยบายการบริหารความเสี่ยงทั่วทั้งองค์กร

2.6 จัดให้มีระบบการบริหารความเสี่ยงให้ครอบคลุมทั่วทั้งองค์กรและแนวทางการปฏิบัติ

2.7 ให้ความมั่นใจในความถูกต้อง ทันเวลาและสอดคล้องกันของข้อมูลของการบริหารความเสี่ยงทั่วทั้งองค์กรต่อคณะกรรมการ และ คณะกรรมการตรวจสอบ

2.8 สร้างวัฒนธรรมการตระหนักต่อการบริหารความเสี่ยงในองค์กร

2.9 ปฏิบัติหน้าที่อื่นใดตามที่คณะกรรมการบริษัทมอบหมาย

2.10 หน้าที่ความรับผิดชอบในฐานะเป็นผู้ดูแลด้านการรักษาความปลอดภัยให้กับโครงสร้างเครือข่ายและความปลอดภัยข้อมูลสารสนเทศ CSO (Chief Security Officer) ซึ่งมีหน้าที่รับผิดชอบดังนี้

1. กำหนดเป้าหมาย นโยบายด้านการรักษาความปลอดภัยข้อมูล โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร (Corporate Strategic Plan)
2. จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยข้อมูล Policy, Standard, Procedure and Guideline เพื่อให้องค์กรได้มาซึ่ง การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคงของระบบ (Availability)
3. จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ โดยใช้ระบบเตือนผู้บุกรุก Intrusion Detection System (IDS), ระบบป้องกันผู้บุกรุก Instrusion Prevention System (IPS) หรือระบบจัดการกำจัดไวรัส (Anti-Virus Systems) ตลอดจนวางแผนเรื่องความต่อเนื่องในการดำเนินธุรกิจและแผนกู้ภัยในสถานการณ์ฉุกเฉิน Business Continuity Plan & Disaster Recovery Plan (BCP and DRP)
4. มีการบริหารความเสี่ยง (Risk Management) และการวิเคราะห์ความเสี่ยง (Risk Analysis) ที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจขององค์กร
5. นำเสนอผู้บริหารระดับสูง(CEO) ในเรื่องของแผนการปฏิบัติงาน นโยบาย งบประมาณ อัตรากำลัง ตลอดจนแผนการ Outsource ด้านความปลอดภัยข้อมูลเพื่อขอดำเนินการอนุมัติและเพื่อให้ผู้บริหารระดับสูงมีความตระหนัก (Awareness) ในความสำคัญเรื่อง Information Security
6. เป็นที่ปรึกษาด้านระบบความปลอดภัยข้อมูลให้กับแผนกอื่นๆ ที่ต้องใช้ IT ในการปฏิบัติงาน
7. ติดต่อและรักษาความสัมพันธ์กับคู่ค้า, องค์กร หรือบุคคลภายนอกที่มีความเกี่ยวข้องกับเรื่องความปลอดภัยข้อมูลทั้งภาครัฐและเอกชนเช่น ตำรวจ, นักข่าว, Systems Integrator (SI), Outsourcer, Managed Security Services Provider (MSSP) และผู้ตรวจสอบ (Auditor)
8. ออกข้อกำหนดในการจัดซื้อจัดจ้างระบบรักษาความปลอดภัยข้อมูลสารสนเทศ Requests for Proposal (RPF)
9. จัดตั้งและควบคุมบริหารทีม Incident Response เพื่อให้สามารถปฏิบัติงานในยามที่เกิดภาวะฉุกเฉินขึ้นในองค์กร เช่น การระบาดของไวรัสคอมพิวเตอร์
10. เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้าน Information Security อย่างสม่ำเสมอ

3. วาระการดำรงตำแหน่ง

คณะกรรมการบริหารความเสี่ยงมีวาระการดำรงตำแหน่งคราวละ 3 ปี และตามวาระการดำรงตำแหน่งของการเป็นกรรมการและ/หรือการดำรงตำแหน่งของการเป็นผู้บริหารของบริษัท ซึ่งเมื่อพ้นจากตำแหน่งตามวาระแล้ว อาจได้รับแต่งตั้งให้กลับเข้าดำรงตำแหน่งได้อีก

4. การประชุมคณะกรรมการบริหารความเสี่ยง

กำหนดให้มีการประชุมคณะกรรมการบริหารความเสี่ยงอย่างน้อยไตรมาสละ 1 ครั้ง

กฎบัตรฉบับนี้ได้รับการอนุมัติจากที่ประชุมสามัญผู้ถือหุ้นประจำปี 2561 เมื่อวันที่ 26 เมษายน 2561

นายจุมพล สำเภาพล

ประธานกรรมการ