กฎบัตรคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ
บริษัท ดับบลิวเอชเอ คอร์ปอเรชั่น จำกัด (มหาชน)

วัตถุประสงค์

บริษัท ดับบลิวเอชเอ คอร์ปอเรชั่น จำกัด (มหาชน) และกลุ่มบริษัท ("**บริษัท**") ได้ตระหนักถึงความสำคัญของการกำกับดูแลกิจการที่ดีว่าเป็นสิ่งสำคัญที่ช่วยส่งเสริมการดำเนินงานของบริษัทให้มีประสิทธิภาพเพื่อการเติบโตที่ยั่งยืนซึ่งจะนำไปสู่ประโยชน์สูงสุดต่อผู้มีส่วนเกี่ยวข้องทุกฝ่าย ตั้งแต่พนักงาน ผู้ลงทุน ผู้ถือหุ้น และผู้มีส่วนได้เสียอื่น ๆ ดังนั้น คณะกรรมการบริษัทจึงเป็นผู้แต่งตั้งคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศและได้กำหนดกฎบัตรคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศฉบับนี้ขึ้น เพื่อให้คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศได้ตระหนักถึงหน้าที่และความรับผิดชอบของตนและปฏิบัติหน้าที่ได้อย่างสมบูรณ์

1. องค์ประกอบคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ

1.1 คณะกรรมการบริษัทเป็นผู้พิจารณาแต่งตั้งกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศโดยมีจำนวนไม่น้อยกว่า 3 คน ทั้งนี้ กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศจะเป็นกรรมการบริษัทหรือไม่ก็ได้

1.2 คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศแต่งตั้งกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศในคณะ 1 ท่านขึ้นดำรงตำแหน่งประธานคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ

1.3 ให้เลขานุการบริษัททำหน้าที่เป็นเลขานุการคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ เพื่อดำเนินงานนัดหมายการประชุม จัดเตรียมวาระการประชุม นำส่งเอกสารประกอบการประชุม และบันทึกรายงานการประชุม

อย่างไรก็ดี คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศอาจพิจารณาแต่งตั้งบุคคลอื่นเพื่อทำหน้าที่เป็นเลขานุการคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศก็ได้

2. คุณสมบัติของคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ

2.1 กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศต้องสามารถอุทิศเวลาอย่างเพียงพอในการปฏิบัติหน้าที่เพื่อให้การดำเนินงานสำเร็จตามวัตถุประสงค์

2.2 กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ต้องเป็นผู้มีความรู้ ความเข้าใจในธุรกิจของบริษัท หรือมีความเชี่ยวชาญเฉพาะด้านที่เป็นปัจจัยต่อการดำเนินธุรกิจของบริษัท และสามารถใช้ดุลยพินิจในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

3. หน้าที่และความรับผิดชอบของคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ

3.1 พิจารณากำหนดนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง ที่สอดคล้องกับวัตถุประสงค์ เป้าหมายหลัก และกลยุทธ์ เพื่อใช้เป็นแนวทางในการปฏิบัติงานในการบริหารความเสี่ยงให้เป็นทิศทางเดียวกันและครอบคลุมทั่วถึงทั้งองค์กร ตลอดจนการบริหารความต่อเนื่องทางธุรกิจ เพื่อนำเสนอต่อคณะกรรมการบริษัทพิจารณาอนุมัติ พร้อมทั้งสอบทาน และทบทวนนโยบายและกรอบการบริหารความเสี่ยงดังกล่าว อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่านโยบายและกรอบการบริหารความเสี่ยง ยังคงสอดคล้องและเหมาะสมกับสภาวะการดำเนินธุรกิจในภาพรวม

3.2 พิจารณากำหนดให้มีการระบุประเด็นและจัดการความเสี่ยงหลักที่สำคัญต่อการดำเนินธุรกิจ (key risk) โดยพิจารณาทั้งปัจจัยภายนอกและภายในที่อาจส่งผลให้บริษัทไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ เช่น ความเสี่ยงด้านกลยุทธ์ (strategic risk) ความเสี่ยงด้านการปฏิบัติงาน (operational risk) ความเสี่ยงอุบัติใหม่ (emerging risk) หรือความเสี่ยงด้านความยั่งยืน (ESG risk) เป็นต้น โดยจัดให้มีผังความเสี่ยงองค์กร (Risk Profile) ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ขององค์กร (Risk Tolerance)

3.3 พิจารณากำกับดูแลเพื่อให้มั่นใจว่าบริษัทได้มีการประเมินผลกระทบและโอกาสที่เกิดขึ้นของความเสี่ยงที่ได้ระบุไว้เพื่อจัดลำดับความเสี่ยงและจัดการความเสี่ยงที่เหมาะสมกับธุรกิจ รวมทั้งพิจารณาให้ความเห็น เสนอแนะ ติดตามมาตรการและแผนปฏิบัติการเพื่อจัดการความเสี่ยงขององค์กร สถานะการบริหารความเสี่ยง และประเมินผลประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงอย่างสม่ำเสมอเพื่อให้มั่นใจว่าองค์กรได้บริหารความเสี่ยงอย่างเพียงพอ เหมาะสม และมีประสิทธิภาพ

3.4 ประสานงานและให้ข้อมูลความเสี่ยงและการควบคุมภายในที่สำคัญแก่คณะกรรมการตรวจสอบ เพื่อให้คณะกรรมการตรวจสอบสามารถพิจารณาให้ความเห็นถึงความเพียงพอของระบบการบริหารความเสี่ยงและการควบคุมภายใน รวมทั้งสามารถนำไปประกอบการพิจารณาอนุมัติแผนการตรวจสอบภายในเพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่าบริษัทมีระบบการควบคุมภายในที่เหมาะสมต่อการจัดการความเสี่ยง รวมทั้งมีการนำระบบบริหารความเสี่ยงมาปรับใช้อย่างเหมาะสมและมีการปฏิบัติทั่วทั้งองค์กร

3.5 ให้คำปรึกษา คำแนะนำ และการสนับสนุนแก่ฝ่ายบริหารและคณะทำงานบริหารความเสี่ยงในเรื่องการบริหารความเสี่ยงขององค์กร รวมถึงส่งเสริมและสนับสนุนให้มีการปรับปรุงพัฒนาระบบและกลไกการบริหารความเสี่ยงภายในองค์กรอย่างต่อเนื่องและสม่ำเสมอเพื่อให้มีวัฒนธรรมการบริหารความเสี่ยงในทุกระดับทั่วทั้งองค์กร โดยมีอำนาจดำเนินการในเรื่องดังต่อไปนี้

(1) ให้ผู้บริหาร ส่วนงาน หรือบุคลากรที่เกี่ยวข้อง ให้ความร่วมมือในการชี้แจงข้อมูลซึ่งเกี่ยวกับการบริหารความเสี่ยง การควบคุมภายใน และการบริหารความต่อเนื่องทางธุรกิจเป็นลายลักษณ์อักษรหรือโดยวาจาผ่านการเข้าร่วมประชุมคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศตามสมควร

(2) สอบทานแผนการบริหารความเสี่ยงองค์กรว่ามีการดำเนินการตรงตามวัตถุประสงค์และสามารถวัดผลได้อย่างเป็นรูปธรรม รวมทั้งให้ข้อเสนอแนะเพิ่มเติมแก่คณะทำงานบริหารความเสี่ยงในสิ่งที่สามารถพัฒนาได้

(3) ติดตามและกำกับดูแลส่วนงานที่เกี่ยวข้องให้ดำเนินการหรือปฏิบัติการอย่างหนึ่งอย่างใดเท่าที่จำเป็น เพื่อให้สามารถปฏิบัติหน้าที่ตามความรับผิดชอบที่ถูกกำหนดไว้ในกฎบัตรหรือตามที่คณะกรรมการบริษัทมอบหมาย

3.6 กำกับดูแลและติดตามการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ (Cybersecurity and Information Security) รวมทั้งระบบจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ตลอดจนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และสารสนเทศ เพื่อให้มั่นใจว่าบริษัทมีระบบและกระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์และสารสนเทศที่มีประสิทธิภาพเพื่อปกป้องข้อมูลและระบบสารสนเทศที่สำคัญ และพร้อมรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและทันท่วงทีเพื่อป้องกันผลกระทบที่อาจเกิดขึ้นต่อบริษัท

3.7 ปฏิบัติงานและภารกิจต่าง ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการบริษัท

3.8 ให้คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศประเมินผลการปฏิบัติงานเป็นประจำทุกปี รวมถึงทบทวนกฎบัตรคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง

3.9 ทั้งนี้ หน้าที่และความรับผิดชอบคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศให้ครอบคลุมถึงบริษัทย่อยที่บริษัทถือหุ้นเกินกว่าร้อยละห้าสิบของจำนวนหุ้นที่มีสิทธิออกเสียงทั้งหมดของบริษัทนั้น โดยไม่รวมบริษัทย่อยที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยและบริษัทย่อยของบริษัทจดทะเบียนนั้น

4. วาระการดำรงตำแหน่ง

4.1 ให้กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศที่เป็นกรรมการบริษัท มีวาระการดำรงตำแหน่งเท่ากับวาระการเป็นกรรมการบริษัท และเมื่อครบวาระการดำรงตำแหน่งดังกล่าว กรรมการที่พ้นจากตำแหน่งตามวาระอาจได้รับการเลือกตั้งให้กลับเข้าดำรงตำแหน่งได้อีก

4.2 ให้กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศที่เป็นผู้บริหารของบริษัท มีวาระการดำรงตำแหน่งเท่าที่ดำรงตำแหน่งเป็นผู้บริหารของบริษัท เว้นแต่คณะกรรมการบริษัทจะมีมติเป็นอย่างอื่น

5. การประชุมคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ

5.1 ให้มีการประชุมคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 4 ครั้ง

5.2 ในการประชุมคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ต้องมีกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศทั้งหมดจึงจะเป็นองค์ประชุม ในกรณีที่ประธานคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศไม่อยู่ในที่ประชุมหรือไม่สามารถปฏิบัติหน้าที่ได้ ให้กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศซึ่งมาประชุมเลือกกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศคนหนึ่งเป็นประธานในที่ประชุม

5.3 การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศคนหนึ่งให้มีหนึ่งเสียงในการลงคะแนน ถ้าคะแนนเสียงเท่ากันให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นการชี้ขาด กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศซึ่งมีส่วนได้เสียในเรื่องใดเรื่องหนึ่งไม่มีสิทธิออกเสียงลงคะแนนในเรื่องนั้น

5.4 ในการเรียกประชุมคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ให้ประธานคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศหรือผู้ซึ่งได้รับมอบหมาย ส่งหนังสือนัดประชุมไปยังกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศไม่น้อยกว่าเจ็ด (7) วันก่อนวันประชุม เว้นแต่ในกรณีจำเป็นรีบด่วนเพื่อรักษาสิทธิและประโยชน์ของบริษัท จะแจ้งนัดประชุมโดยวิธีอื่นและกำหนดวันประชุมให้เร็วกว่านั้นก็ได้ ในกรณีที่เป็นการประชุมผ่านสื่ออิเล็กทรอนิกส์ การส่งหนังสือเชิญประชุมจะส่งผ่านสื่ออิเล็กทรอนิกส์ก็ได้

5.5 เมื่อสิ้นสุดการประชุม เลขานุการคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศเป็นผู้มีหน้าที่จัดทำรายงานการประชุม และจัดส่งให้ประธานคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศพิจารณาลงลายมือชื่อรับรองความถูกต้อง โดยเสนอให้ที่ประชุมรับรองในการประชุมครั้งถัดไป ทั้งนี้ กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศสามารถแสดงความคิดเห็นขอแก้ไขเพิ่มเติมรายงานการประชุมให้มีความละเอียดถูกต้องมากที่สุดได้

6. การรายงาน

ให้คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศรายงานผลการปฏิบัติงานให้คณะกรรมการบริษัทเพื่อรับทราบเป็นประจำ ทั้งนี้ ในกรณีที่มีปัจจัยหรือเหตุการณ์สำคัญซึ่งอาจส่งผลกระทบต่อบริษัทอย่างมีนัยสำคัญ ต้องรายงานต่อคณะกรรมการบริษัทเพื่อทราบและพิจารณาโดยเร็ว

ให้คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศจัดทำรายงานผลการปฏิบัติงานและเปิดเผยไว้ในรายงานประจำปี และ/หรือ แบบ 56-1 One Report เช่น จำนวนครั้งที่ประชุมในรอบปี สถิติการเข้าประชุม และผลการปฏิบัติหน้าที่ เป็นต้น

7. ค่าตอบแทน

ให้กรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศได้รับค่าตอบแทนตามที่ที่ประชุมผู้ถือหุ้นอนุมัติ

กฎบัตรคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 6/2568 เมื่อวันที่ 14 พฤศจิกายน 2568 โดยให้มีผลใช้บังคับตั้งแต่วันที่ 15 พฤศจิกายน 2568 เป็นต้นไป

(นายสมคิด จาตุศรีพิทักษ์)
ประธานคณะกรรมการบริษัท