ประกาศ
ที่ 9/2568
เรื่อง “นโยบายความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Policy)”

---

1. บทนำ

บริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด (“บริษัทฯ”) มุ่งมั่นในการสร้างความเชื่อมั่นและความไว้วางใจแก่ลูกค้า ผ่านการให้บริการด้านการบริหารจัดการระบบสารสนเทศ (IT Infrastructure) และการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Managed Security Services) ที่มีคุณภาพ เชื่อถือได้ และปลอดภัย บริษัทฯ ตระหนักว่าความมั่นคงปลอดภัยไซเบอร์ไม่ใช่เพียงความรับผิดชอบทางเทคนิค แต่เป็นองค์ประกอบเชิงกลยุทธ์ที่สำคัญซึ่งมีผลโดยตรงต่อความสำเร็จทางธุรกิจ ความไว้วางใจของลูกค้า การปกป้องข้อมูลสารสนเทศอันเป็นสินทรัพย์ล้ำค่า และการเติบโตอย่างยั่งยืนขององค์กร

เพื่อให้บรรลุเป้าหมายเชิงกลยุทธ์และตอบสนองต่อความคาดหวังของผู้มีส่วนได้ส่วนเสียทุกฝ่าย บริษัทฯ ได้จัดตั้งโครงสร้างองค์กรสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน โดยกำหนดบทบาทและหน้าที่ของคณะกรรมการบริหาร ผู้บริหารระดับสูง บุคลากรทุกระดับ คู่ค้า และพันธมิตรทางธุรกิจ ภายใต้กรอบการดำเนินงานที่ใช้มาตรฐานสากล เช่น ISO/IEC 27001 และ NIST Cybersecurity Framework (CSF) Version 2.0 ครอบคลุมทั้ง 6 ฟังก์ชันหลัก ได้แก่ การกำกับดูแล (Govern), การระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond) และการฟื้นฟู (Recover) พร้อมสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กฎหมายและข้อบังคับที่เกี่ยวข้อง

นโยบายความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ ได้รับการกลั่นกรองจากคณะกรรมการ และได้รับการอนุมัติจากผู้บริหารระดับสูงของบริษัทฯ เพื่อเป็นรากฐานสำคัญในการกำหนดทิศทางและความคาดหวังด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการบริหารความเสี่ยงให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) นโยบายนี้ยังมุ่งเน้นการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง การบริหารจัดการความเสี่ยงจากห่วงโซ่อุปทาน (Supply Chain) และการกำกับดูแล ติดตาม ทบทวน และปรับปรุงอย่างต่อเนื่อง เพื่อให้มาตรการต่าง ๆ มีความเหมาะสม ทันสมัย และสามารถรับมือกับภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงตลอดเวลาได้อย่างมีประสิทธิภาพ

2.วัตถุประสงค์

2.1. เพื่อให้มั่นใจว่าการให้บริการด้าน IT Infrastructure และ Managed Security Services ของบริษัทฯ มีความมั่นคงปลอดภัยสูงสุด ด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศ (Confidentiality, Integrity, Availability) และระบบที่เป็นสินทรัพย์สำคัญของลูกค้าและองค์กรจากการเข้าถึง การเปิดเผย การดัดแปลงแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต

2.2. เพื่อกำหนดและนำกรอบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน NIST Cybersecurity Framework (CSF) Version 2.0 มาปรับใช้อย่างเป็นระบบทั่วทั้งองค์กร ครอบคลุมการกำกับดูแล (Govern) การระบุ (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการฟื้นฟู (Recover) เพื่อยกระดับความสามารถในการรับมือกับความเสี่ยงทางไซเบอร์

2.3. เพื่อกำกับดูแลและบริหารความเสี่ยงไซเบอร์ให้สอดคล้องกับกลยุทธ์ธุรกิจ ระดับความเสี่ยงที่ยอมรับได้ และกฎหมายที่เกี่ยวข้อง พร้อมมีกลไกติดตามและปรับปรุงอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามาตรการความมั่นคงปลอดภัยมีประสิทธิภาพและทันต่อภัยคุกคามที่เปลี่ยนแปลง

2.4. เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของบริษัทฯ สอดคล้องกับกฎหมาย ข้อบังคับ มาตรฐาน และข้อผูกพันตามสัญญาที่เกี่ยวข้อง รวมถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อกำหนดเฉพาะของลูกค้า

2.5. เพื่อให้บริษัทฯ สามารถตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ลดผลกระทบต่อการดำเนินธุรกิจ การให้บริการ และความเชื่อมั่นของลูกค้า

2.6. เพื่อส่งเสริมการมีส่วนร่วมของผู้บริหาร บุคลากรทุกระดับ คู่ค้า และพันธมิตรทางธุรกิจ ในการรับรู้และปฏิบัติตามแนวทางความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

3. กลยุทธ์การจัดการด้านไซเบอร์

เพื่อให้การดำเนินงานของบริษัทเป็นไปอย่างมั่นคงปลอดภัย สอดคล้องกับมาตรฐานสากล และสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการ ลูกค้า และคู่ค้า บริษัทฯ กำหนดกลยุทธ์ในการจัดการด้านไซเบอร์ (Cybersecurity Management Strategy) ดังต่อไปนี้

3.1. การประเมินความเสี่ยงอย่างต่อเนื่อง (Continuous Risk Assessment)

บริษัทฯ ดำเนินการประเมินภัยคุกคามและความเสี่ยงที่เกี่ยวข้องกับการให้บริการอย่างสม่ำเสมอ โดยจัดลำดับความสำคัญตามระดับผลกระทบและความเป็นไปได้ เพื่อให้สามารถออกแบบและดำเนินมาตรการป้องกันได้อย่างเหมาะสมและมีประสิทธิภาพ

3.2. การป้องกันเชิงรุก (Proactive Protection)

บริษัทฯ นำเทคโนโลยีและเครื่องมือที่ทันสมัยมาใช้ เช่น Threat Intelligence, SIEM, SOAR และ Next-Gen Firewall เพื่อเสริมสร้างความสามารถในการป้องกันภัยคุกคาม รวมถึงติดตามพัฒนาการของภัยคุกคามใหม่ๆ และปรับปรุงมาตรการป้องกันให้สอดคล้องอย่างต่อเนื่อง

3.3. การตรวจจับและตอบสนองต่อเหตุการณ์ (Detection and Response)

บริษัทฯ จัดตั้งศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) ที่สามารถตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงได้ตลอด 24 ชั่วโมงทุกวัน พร้อมทั้งพัฒนา Playbook สำหรับการตอบสนองเหตุการณ์ และจัดให้มีการซ้อมเหตุการณ์จำลอง (Cyber Drill) อย่างน้อยปีละ 1 ครั้ง

3.4. การบริหารจัดการช่องโหว่ (Vulnerability Management)

บริษัทฯ ดำเนินการตรวจสอบและจัดการช่องโหว่ทั้งในระบบที่ใช้ในการบริหารจัดการลูกค้าและระบบภายในองค์กรอย่างสม่ำเสมอ โดยจัดทำแผนแก้ไข (Remediation Plan) ที่ชัดเจน และติดตามความคืบหน้าจนกว่าจะแก้ไขสำเร็จ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ดังกล่าว

3.5. การพัฒนาทักษะและศักยภาพของบุคลากร

บริษัทฯ จัดให้มีการฝึกอบรมและพัฒนาทักษะด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคลากรทุกระดับอย่างต่อเนื่อง เพื่อสร้างความตระหนักรู้และความเข้าใจถึงบทบาทและหน้าที่ของแต่ละบุคคลในการปกป้องทรัพยากรสารสนเทศของบริษัทฯ

3.6. การปฏิบัติตามกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง

บริษัทฯ ปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องในประเทศไทย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงดำเนินการตามมาตรฐานสากล เช่น ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 20000-1 และ NIST Cybersecurity Framework เพื่อให้มั่นใจว่ากระบวนการด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามหลักปฏิบัติที่ดีที่สุด

4. ขอบเขตการบังคับใช้

นโยบายนี้ครอบคลุมถึงสินทรัพย์ด้านสารสนเทศทั้งหมดของบริษัทฯ ซึ่งรวมถึงระบบเทคโนโลยีสารสนเทศ โครงสร้างพื้นฐาน ข้อมูล รวมถึงเจ้าหน้าที่ของบริษัท คู่ค้าและพันธมิตรทางธุรกิจที่ร่วมกันดำเนินกิจกรรมทางธุรกิจ และบุคลากรที่เกี่ยวข้องทั้งภายในและภายนอกที่ทำงานหรือเข้าถึงทรัพยากรของบริษัทฯ

5. การกำกับดูแลและบทบาทความรับผิดชอบ

บริษัทฯ มีการกำหนดโครงสร้าง และหน้าที่ในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ มีการแบ่งแยกออกเป็น 3 ระดับ ตามแนวคิด “แนวป้องกันสามด่าน” (Three Lines of Defense) มีดังนี้

(1) ระดับที่ 1 (First line of defense) : หน่วยงานปฏิบัติการ ดำเนินการภายใต้นโยบายความมั่นคงปลอดภัยไซเบอร์ กำกับดูแล เฝ้าระวัง ป้องกัน ตรวจสอบ ทรัพย์สินสารสนเทศและระบบที่เกี่ยวข้อง รวมถึงปฏิบัติตามแผนรับมือกับเหตุการณ์ต่างๆ และกู้คืนข้อมูลเพื่อให้การดำเนินการทางธุรกิจเป็นไปอย่างต่อเนื่อง

(2) ระดับที่ 2 (Second line of defense) : หน่วยงานบริหารความเสี่ยงและกำกับดูแลการ ปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงให้คำแนะนำด้านการควบคุมความเสี่ยง กำกับดูแล และติดตามการปฏิบัติตามนโยบาย กฎหมาย และข้อบังคับต่างๆ

(3) ระดับที่ 3 (Third line of defense) : หน่วยงานตรวจสอบ มีบทบาทหลักในการเป็นผู้ที่ให้การตรวจสอบและให้ความเชื่อมั่นอย่างเป็นอิสระและเที่ยงธรรมต่อประสิทธิผลของการบริหารจัดการความเสี่ยงและมาตรการควบคุมของระดับ 1 และระดับ 2

6. การระบุและจัดการทรัพย์สิน (Asset Management)

บริษัทฯ มีการระบุ จัดทำบัญชี จัดประเภท มอบหมายความเป็นเจ้าของ ของทรัพย์สินสารสนเทศ ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ และระบบต่างๆ โดยมีการบริหารจัดการอย่างเหมาะสมตลอดวงจรชีวิตตั้งแต่การจัดหา การใช้งาน จนถึงการทำลายหรือเลิกใช้งาน โดยยึดปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศและข้อมูลส่วนบุคคล (Information security and privacy policy) รวมถึงแนวทางของ NIST CSF 2.0 ดังนี้

6.1. การจัดทำบัญชีทรัพย์สิน (Asset identification and inventory)

6.2. การจัดประเภทข้อมูลและทรัพย์สิน (Information and asset classification)

6.3. การจัดทำป้าย (Labeling)

6.4. การกำหนดเจ้าของทรัพย์สิน (Ownership)

6.5. การจัดการวงจรชีวิตทรัพย์สิน (Asset Lifecycle Management) จะต้องมีการปฏิบัติงาน ดังนี้

- **การอนุญาตให้ใช้ทรัพย์สินขององค์กร (Acceptable Use Policy):** ผู้ใช้งานทุกคนต้องปฏิบัติตามกฎเกณฑ์และเงื่อนไขการใช้งานข้อมูลและทรัพย์สินสารสนเทศที่เกี่ยวข้อง ตามที่ระบุในนโยบายความมั่นคงปลอดภัยสารสนเทศ เรื่อง นโยบายการอนุญาตให้ใช้ทรัพย์สินขององค์กร
- **การส่งคืนทรัพย์สิน (Return of Assets):** เมื่อสิ้นสุดการจ้างงาน สัญญา หรือข้อตกลง บุคลากรทุกคนและผู้มีส่วนได้ส่วนเสียภายนอกที่เกี่ยวข้อง จะต้องส่งคืนทรัพย์สินทั้งหมดขององค์กรที่อยู่ในความครอบครอง
- **การลบข้อมูล (Information Deletion):** ข้อมูลที่จัดเก็บในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูลใด ๆ จะต้องถูกลบหรือทำลายอย่างปลอดภัยเมื่อไม่จำเป็นต้องใช้งานอีกต่อไป เพื่อป้องกันการรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต

7. การประเมินและบริหารจัดการความเสี่ยงทางไซเบอร์ (Risk Assessment and Management)

บริษัทฯ ดำเนินการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงทางไซเบอร์ และจัดระดับความเสี่ยงทางไซเบอร์ที่เผชิญอยู่ และกำหนดแนวทางการตัดสินใจในการเลือกแนวทางการจัดการความเสี่ยงที่เหมาะสม เพื่อลดโอกาสและผลกระทบจากภัยคุกคามให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) และสอดคล้องกับกลยุทธ์การบริหารจัดการความเสี่ยง (GV.RM) และกระบวนการประเมินความเสี่ยง (ID.RA) ตามแนวทางของ NIST CSF 2.0 บริษัทฯ จึงได้กำหนดให้ต้องดำเนินการดังนี้

7.1. กลยุทธ์และกระบวนการบริหารจัดการความเสี่ยง (Risk Management Strategy and Process)

7.2. การระบุและวิเคราะห์ความเสี่ยง (Risk Identification and Analysis)

7.3. การประเมินและแผนการจัดการความเสี่ยง (Risk Evaluation and Treatment Plan)

7.4. การยอมรับความเสี่ยงคงเหลือและการสื่อสาร (Residual Risk Acceptance and Communication)

7.5. การทบทวนและติดตามความเสี่ยง (Risk Review and Monitoring)

8. การป้องกัน (Protection)

มีการกำหนดมาตรการป้องกัน (Protective Measures) ที่เหมาะสม โดยคำนึงถึงความพร้อมใช้งาน (Availability) ความถูกต้องครบถ้วน (Integrity) และความลับ (Confidentiality) ของข้อมูลและระบบสารสนเทศที่สำคัญขององค์กร มาตรการเหล่านี้มีจุดมุ่งหมายเพื่อจำกัดหรือยับยั้งผลกระทบจากเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และดำเนินการนำไปปฏิบัติในทุกฝ่ายที่เกี่ยวข้องตามขอบเขตที่ระบุในนโยบายนี้ บริษัทฯ จึงได้กำหนดให้ต้องดำเนินการดังนี้

8.1. การควบคุมการเข้าถึง (Access Control)

มีบังคับใช้นโยบายและกระบวนการควบคุมการเข้าถึง เพื่อให้ผู้ใช้งานจะสามารถเข้าถึงได้เฉพาะข้อมูลและระบบที่จำเป็นต่อการปฏิบัติงานตามหน้าที่ความรับผิดชอบ (Principle of Least Privilege) และมีการจัดการอัตลักษณ์ (Identity Management) มีการพิสูจน์ตัวตนอย่างปลอดภัย (Secure authentication) การจัดการสิทธิ์การเข้า (Access right) และสิทธิ์ระดับสูง (Privileged access right) ที่รัดกุมและเหมาะสมกับระดับความเสี่ยง

8.2. ความตระหนักรู้และการฝึกอบรม (Awareness and Training)

มีจัดการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมและต่อเนื่อง แก่บุคลากรทุกคน รวมถึงผู้ที่เกี่ยวข้อง เพื่อให้บุคลากรมีความเข้าใจในนโยบาย ขั้นตอนปฏิบัติ ภัยคุกคามที่เกี่ยวข้อง และสามารถปฏิบัติงานได้อย่างมั่นคงปลอดภัย

8.3. ความปลอดภัยของข้อมูล (Data Security)

บริษัทฯ มีการจัดระดับความสำคัญของข้อมูลเพื่อดำเนินการปกป้อง รักษาความลับ รักษาความถูกต้องครบถ้วน และต้องมีความพร้อมใช้งานของข้อมูลตลอดวงจรชีวิต (Data Lifecycle) ตั้งแต่การสร้างหรือรับเข้า การจัดเก็บ การประมวลผล การส่งต่อ การเก็บรักษา จนถึงการทำลาย เป็นไปตามความเหมาะสมกับระดับความสำคัญ โดยดำเนินการเข้ารหัสข้อมูล (Cryptography) การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention) การสำรองข้อมูล (Backup) และการจัดการสื่อบันทึกข้อมูลอย่างปลอดภัย

8.4. การบำรุงรักษาระบบ (System Maintenance)

บริษัทฯ มีกระบวนการบำรุงรักษาระบบสารสนเทศ ฮาร์ดแวร์ และซอฟต์แวร์ ตามรอบระยะเวลาบำรุงรักษาโดยเริ่มตั้งแต่การติดตั้งซอฟต์แวร์บนระบบสารสนเทศ (Installation of software on operational systems), การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities) เช่น การติดตั้งโปรแกรมแก้ไขช่องโหว่ (Patch Management) และการบริหารจัดการการตั้งค่าความปลอดภัยของระบบ (Configuration Management) เพื่อลดความเสี่ยงจากการมีช่องโหว่ที่อาจถูกโจมตี

8.5. เทคโนโลยีป้องกัน (Protective Technology)

บริษัทฯ นำเทคโนโลยีป้องกันที่เหมาะสมและทันสมัยสำหรับแต่ละด้าน เพื่อเสริมสร้างความแข็งแกร่งในการป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยมีศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) และทีมงานที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงในแต่ละด้าน บริหารจัดการเทคโนโลยีที่นำมาใช้เพื่อให้เกิดประสิทธิภาพสูงสุดและตอบสนองต่อภัยคุมคามต่างๆ ได้ทันถ่วงที

9. การตรวจจับ (Detection)

มีการกำหนดกระบวนการ เครื่องมือ และเทคโนโลยีที่เหมาะสม ในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Events) และกิจกรรมที่ผิดปกติ (Anomalies) ที่เกิดขึ้นภายในระบบสารสนเทศ เครือข่าย และทรัพย์สินที่เกี่ยวข้องขององค์กร โดยมีศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) ที่สามารถตรวจจับ วิเคราะห์และตอบสนองต่อเหตุการณ์ด้านความมั่นคง รวมถึงทีมงานผู้เชี่ยวชาญดำเนินการตลอด 24 ชั่วโมง 7 วัน ทำให้สามารถตรวจจับและติดตามภัยคุกคามต่างๆ ได้อย่างต่อเนื่อง มีประสิทธิภาพ และทันท่วงที การตรวจจับที่รวดเร็วและแม่นยำเป็นสิ่งสำคัญเพื่อให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้อย่างเหมาะสม

10. การตอบสนองต่อเหตุการณ์ภัยคุกคาม (Incident Response)

บริษัทฯ มีการกำหนดโครงสร้างทีมงานของผู้ที่เกี่ยวข้องพร้อมกำหนดอำนาจหน้าที่ของแต่ละส่วนงานเพื่อให้สามารถดำเนินงานและปฏิบัติตามขั้นตอนที่มีการวางแผน จัดเตรียม ได้อย่างมีประสิทธิภาพ และตอบสนองต่อเหตุการณ์ภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น เพื่อจำกัดความเสียหายและผลกระทบต่อการดำเนินงาน ทรัพย์สิน และชื่อเสียงขององค์กร ฟื้นฟูระบบและบริการให้กลับสู่สภาวะปกติโดยเร็วที่สุด มีการสื่อสารกับผู้มีส่วนได้รับผลกระทบในทุกส่วนอย่างเหมาะสม และนำบทเรียนที่ได้รับมาปรับปรุงมาตรการความมั่นคงปลอดภัยอย่างต่อเนื่อง โดยมีการทบทวนและซักซ้อมการดำเนินการอย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงตามความเหมาะสม

11. การกู้คืน (Recover)

บริษัทฯ กำหนดให้มีการสำรองและกู้คืนข้อมูล (Data Backup and Restoration) โดยการวางแผน กำหนดขั้นตอนกระบวนการและวิธีดำเนินการในการฟื้นฟู (Resilience) ที่เหมาะสม เพื่อให้สามารถกู้คืนระบบสารสนเทศ ข้อมูล และการดำเนินงานที่สำคัญได้อย่างรวดเร็วและมีประสิทธิภาพภายหลังจากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์หยุดชะงักอื่น ๆ ที่ส่งผลกระทบรุนแรง ทั้งนี้ เพื่อลดผลกระทบต่อการดำเนินธุรกิจ รักษาความต่อเนื่องในการให้บริการ และรักษาความพร้อมใช้งานตามข้อตกลงระดับการให้บริการ (Service Level Agreement) และมีการสื่อสารกับผู้ที่เกี่ยวข้องอย่างเหมาะสม โดยมีการทบทวนและซักซ้อมการดำเนินการอย่างน้อย 1 ครั้งต่อปี

12. การจัดการความเสี่ยงของห่วงโซ่อุปทาน (Supply Chain Risk Management)

มีการกำหนดกรอบการดำเนินงานและแนวทางปฏิบัติที่เป็นระบบในการระบุ ประเมิน จัดการ และติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นจากหรือผ่านทางคู่ค้า ผู้ให้บริการภายนอก และผู้มีส่วนเกี่ยวข้องอื่น ๆ ในห่วงโซ่อุปทาน (Supply Chain) ของบริษัทฯ ทั้งนี้ เพื่อลดโอกาสและผลกระทบจากภัยคุกคามที่อาจส่งผลต่อข้อมูล ทรัพย์สิน ระบบ และการดำเนินงานของบริษัทฯ จึงได้กำหนดให้ต้องดำเนินการดังนี้

12.1. มีกระบวนการจัดการความเสี่ยงของห่วงโซ่อุปทาน (Supply Chain Risk Management Process)

มีกระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ปฏิบัติอย่างต่อเนื่อง ครอบคลุมตลอดระยะเวลาที่ดำเนินธุรกิจกับคู่ค้าและผู้ให้บริการภายนอก ตั้งแต่ขั้นตอนการประเมินและคัดเลือก การทำสัญญา การเริ่มต้นใช้บริการ/รับมอบผลิตภัณฑ์ การดำเนินงาน การติดตามและทบทวน จนถึงการสิ้นสุดสัญญา

12.2. มีการระบุและประเมินความเสี่ยงของคู่ค้าและผู้ให้บริการ (Supplier and Vendor Risk Identification and Assessment)

มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของคู่ค้าและผู้ให้บริการทั้งก่อนเริ่มความร่วมมือหรือดำเนินการและประเมินซ้ำตามรอบระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

12.3. มีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในข้อตกลง (Security Requirements in Agreements)

มีข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน เหมาะสม และสามารถบังคับใช้ได้ จัดทำเป็นข้อตกลงหรือสัญญากับคู่ค้าและผู้ให้บริการ

12.4. มีการจัดการความมั่นคงปลอดภัยในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Supply Chain Security)

มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับคู่ค้าและผู้ให้บริการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ทั้ง ผลิตภัณฑ์ ซอฟต์แวร์ หรือบริการที่อาจมีผลกระทบสูงต่อความมั่นคงปลอดภัยของระบบและข้อมูลขององค์กร ตลอดระยะเวลาที่ใช้งานผลิตภัณฑ์ ซอฟต์แวร์ หรือบริการนั้น

12.5. มีการติดตาม ทบทวน และจัดการการเปลี่ยนแปลงของบริการจากคู่ค้า/ผู้ให้บริการ (Monitoring, Review, and Change Management of Supplier Services)

มีการติดตาม ทบทวน และจัดการการเปลี่ยนแปลงของบริการจากคู่ค้า/ผู้ให้บริการ อย่างสม่ำเสมอตามระดับความเสี่ยงที่ประเมินได้ รวมถึงการจัดการการเปลี่ยนแปลงในบริการหรือสภาพแวดล้อมของคู่ค้า/ผู้ให้บริการที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของบริษัท

13. การทบทวนและปรับปรุงนโยบาย (Policy Review and Updates)

มีการทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์ของบริษัทฯ รวมถึงนโยบายย่อย ขั้นตอนปฏิบัติ และเอกสารที่เกี่ยวข้องทั้งหมด ให้มีความเหมาะสม (Suitability) เพียงพอ (Adequacy) และมีประสิทธิผล (Effectiveness) ในการสนับสนุนวัตถุประสงค์ทางธุรกิจ การจัดการความเสี่ยง และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องอย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง หรือ เกิดปัจจัยกระตุ้นที่สำคัญ (Significant Triggers) และมีการสื่อสารไปยังบุคลากรทุกคนและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างทั่วถึง เพื่อให้ทุกคนได้รับทราบ เข้าใจ และสามารถปฏิบัติตามการเปลี่ยนแปลงและข้อกำหนดใหม่ได้อย่างถูกต้อง

14. การปฏิบัติตามนโยบาย

พนักงานทุกคนและผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด หากพบว่ามีการละเมิดนโยบาย จะถูกพิจารณาทางวินัยตามข้อบังคับของบริษัท หรือกฎหมายที่เกี่ยวข้อง

ประกาศ ณ วันที่ 1 สิงหาคม 2568

(นายอรรถวุฒิ คำประดิษฐ์)
กรรมการผู้จัดการ
บริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด