ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

---

1. วัตถุประสงค์

- เพื่อเป็นกรอบแนวทางการปฏิบัติงานขององค์กรในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- เพื่อรับมือกับภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกองค์กรที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท
- เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้พนักงานปฏิบัติตามได้อย่างถูกต้อง เหมาะสม และเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- เพื่อเป็นแนวทางบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั้งจากภายในและภายนอกองค์กร
- เพื่อเป็นกรอบแนวทางให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของ ธพส. ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้เหมาะสม

2. ขอบเขตและการบังคับใช้

ขอบเขตของนโยบายนี้ครอบคลุมการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับวัตถุประสงค์การดำเนินงานตามภารกิจของ ธพส. ที่ส่งเสริมให้พนักงานทุกคนต้องตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีผลบังคับใช้ไปถึงบุคลากรหรือหน่วยงานภายในทั้งหมด ได้แก่ กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ พนักงานและลูกจ้างของ ธพส. ผู้มีส่วนได้ส่วนเสีย

3. ข้อยกเว้น

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้นโดยปฏิบัติตามขั้นตอนการยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของหน่วยงานร่วมด้วย

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

4. บทบาทและความรับผิดชอบ

บทบาทและความรับผิดชอบกำหนดตามตารางต่อไปนี้

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	• ทำหน้าที่พิจารณากลั่นกรอง กำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีดิจิทัล
กรรมการผู้จัดการ	กรรมการผู้จัดการ	• ทำหน้าที่กำหนดและส่งเสริมนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy) • สนับสนุนให้มีการดำเนินธุรกิจของบริษัทเป็นไปตามนโยบาย
ผู้บริหาร	รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ ผู้อำนวยการฝ่ายที่เกี่ยวข้อง หรือพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วนหรือผู้ชำนาญการขึ้นไป	• สนับสนุนเพื่อขับเคลื่อนการดำเนินงานโดยจัดให้มีกลยุทธ์ เป้าหมาย แผนงาน รวมถึงโครงสร้างผู้รับผิดชอบ เพื่อเป็นผู้แทนผู้บริหารในการดำเนินงาน เช่น คณะกรรมการ คณะทำงาน หน่วยงาน ผู้รับผิดชอบ เป็นต้น • สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุง การปฏิบัติงานอย่างต่อเนื่อง • ส่งเสริม สนับสนุนความรู้ ปลูกจิตสำนึกและสร้างวัฒนธรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy) รวมถึงปฏิบัติตนให้เป็นแบบอย่างแก่พนักงาน • ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลดำเนินงานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy) ก่อนนำเสนอคณะกรรมการ
พนักงาน	พนักงานทุกคนภายใน ธพส.	• ศึกษา ทำความเข้าใจเกี่ยวกับนโยบายและเป้าหมาย การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy) • รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

5. คำนิยาม

"บริษัท" หมายถึง บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด หรือเรียกโดยย่อว่า ธพส.

"คณะกรรมการ" หมายถึง คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล

"ผู้บริหาร" หมายถึง กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ ผู้อำนวยการฝ่ายที่เกี่ยวข้อง และพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วน หรือผู้ชำนาญการขึ้นไป

"พนักงาน" หมายถึง บุคคลที่บริษัทตกลงว่าจ้างให้เข้ามาทำงานเป็นการประจำ หรือตามสัญญาจ้างที่มีกำหนดระยะเวลาให้แก่บริษัท โดยได้รับเงินเดือนหรือค่าจ้าง ยกเว้นกรรมการผู้จัดการ ตามพระราชบัญญัติคุ้มครองแรงงานฯ และพนักงานรัฐวิสาหกิจ พ.ศ. 2518 และที่แก้ไขเพิ่มเติม และรองกรรมการผู้จัดการที่มาจากสัญญาจ้าง

"หน่วยงานรับผิดชอบ" หมายถึง คณะทำงาน คณะกรรมการฝ่ายงาน กลุ่มงานของ ธพส. ที่รับผิดชอบในการพัฒนาระบบบริหารจัดการ และระบบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานตามนโยบาย

"ผู้มีส่วนได้ส่วนเสีย" หมายถึง บุคคลหรือกลุ่มที่มีความสนใจหรือได้รับผลกระทบจากการดำเนินงานขององค์กร ทั้งภายใน เช่น ผู้บริหาร พนักงาน และผู้ถือหุ้น และภายนอก เช่น ลูกค้า คู่ค้า หน่วยงานรัฐ และสังคม

"ระบบคอมพิวเตอร์ (Computer System)" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์ การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้งและยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท

"ข้อมูลสารสนเทศ (Information Technology)" หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือหรืออุปกรณ์ใด ๆ

"ข้อมูลสำคัญ" หรือ **"ข้อมูลที่เป็นความลับ (Sensitive Information)"** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัทหรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมายจรรยาบรรณ ในการประกอบธุรกิจหรือสัญญาซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่นหรือนำไปใช้ประโยชน์อย่างอื่นนอก เหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญหรือข้อมูลที่เป็นความลับดัง กล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงักขาดประสิทธิภาพหรือบริษัทเสื่อมเสียชื่อเสียง

เลขที่ ๑๒๐ อาคารธนทิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๙๙๙๙ www.dad.co.th

"ระบบที่มีความสำคัญ (Important System)" หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทให้เป็นปกติและระบบที่ได้รับการกำหนดโดยหน่วยงาน ด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการ ทำงานหรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงักหรือด้อยประสิทธิภาพ

"Remote Access" หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบภายในเครือข่ายของบริษัทจากระบบเครือข่ายภายนอกบริษัท (Internet)

"เจ้าของระบบ (System Owner)" หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้น ๆ

"ผู้อารักขา (Custodian)" หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการและควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด

"ผู้ดูแลระบบ (Administrator)" หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัททำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย

"การรักษาความมั่นคงปลอดภัย" หรือ **"ความมั่นคงปลอดภัย (Security)"** หมายถึง กระบวนการและ การกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน การดูแลรักษาระบบคอมพิวเตอร์และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญให้พ้นจากความพยายามใด ๆ ทั้งจากพนักงานภายในและจากบุคคลภายนอก ในการเข้าถึงเพื่อโจรกรรมทำลายหรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัทได้รับความเสียหาย

"บุคคลภายนอก (External Party)" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น

- บริษัทคู่ค้า (Business Partner)
- ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
- ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier)
- ผู้ให้บริการต่าง ๆ (Service Provider)
- ที่ปรึกษา (Consultant)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

6. นโยบายและข้อปฏิบัติ

หลักสำคัญหรือหัวใจของการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Principles)

หลักการปฏิบัติที่เป็นหัวใจของการรักษาความมั่นคงปลอดภัยไซเบอร์ มีหลักการสำคัญเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้ (หลัก CIA-AAA-N)

1. การรักษาชั้นความลับ (Confidentiality) การปกป้องและการรักษาชั้นความลับของข้อมูลโดยเป็นการป้องกันการเข้าถึงข้อมูลหรือป้องกันการเปิดเผยข้อมูลต่าง ๆ ที่อาจจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัทจากผู้ที่ไม่ได้รับอนุญาต

2. ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) การรักษาความถูกต้องของข้อมูลที่อยู่ในการควบคุมเพื่อทำให้มั่นใจได้ว่าข้อมูลทั้งหมดไม่มีการแก้ไข ดัดแปลง หรือถูกทำลายจากผู้ที่ไม่ได้รับอนุญาต

3. ความพร้อมใช้งาน (Availability) การทำให้ผู้ได้รับอนุญาตสามารถใช้งานระบบเครือข่ายข้อมูลหรือบริการที่องค์กรมี ได้อย่างรวดเร็ว เชื่อถือได้ และมีความพร้อมใช้งานตลอดเวลา

4. ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบในการทำงานตามหน้าที่งานของแต่ละบุคคล แผนกฝ่าย และผู้บริหาร โดยการรับผิดชอบนี้ รวมถึงการรับผิดและรับชอบในผลของการกระทำตามบทบาทหน้าดังกล่าว นอกจากนี้ความรับผิดชอบสำหรับองค์กรต้องมีระบบที่เจ้าหน้าที่สามารถตรวจสอบและสืบค้นได้ว่าบุคคลใดในองค์กรเป็นผู้รับผิดชอบการกระทำนั้น ๆ

5. การยืนยันตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าถึงและการเข้าใช้งานระบบเครือข่ายข้อมูล หรือบริการทางสารสนเทศที่องค์กรมีทั้งหมดต้องผ่านกระบวนการยืนยันตัวตนที่ถูกต้องและสมบูรณ์แล้วเท่านั้น รวมถึงการเก็บข้อมูลผู้ใช้งานระบบที่มีความเกี่ยวข้องทั้งหมด

6. การกำหนดสิทธิการเข้าถึงที่เหมาะสม (Authorization) การกำหนดสิทธิการเข้าถึงหรือการเข้าใช้งานระบบ เครือข่าย ข้อมูล หรือบริการสารสนเทศที่องค์กรมีทั้งหมดให้อย่างน้อยเป็นไปตามความจำเป็นเท่าที่ผู้ที่ได้รับอนุญาตสามารถทำงานได้ (Least privilege basis) และให้อย่างน้อยเป็นไปตามความต้องการพื้นฐานสำหรับการทำงานตามที่ได้รับอนุญาตเท่านั้น (Need to know basis)

7. การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น โดยการใช้หลักฐานที่องค์กรสามารถหาได้จากระบบ เครือข่าย ข้อมูล หรือบริการสารสนเทศที่องค์กรมี อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยไซเบอร์จะมีประสิทธิภาพและประสิทธิผลนั้น จำเป็นต้องมีข้อตกลงร่วมกันในองค์กรและได้รับความเอาใจใส่อย่างจริงจังจากบุคลากรทุกแผนกฝ่าย และเจ้าหน้าที่ทุกคนในองค์กรในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

7.1. การรักษาความมั่นคงปลอดภัยไซเบอร์ถือว่าเป็นหน้าที่ของพนักงานและบุคคลที่เกี่ยวข้องกับองค์กรทั้งหมด

7.2. การบริหารและการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

7.3. การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่าง ๆ ถือเป็นสิ่งที่สำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์

7.4. การอธิบายให้พนักงานและบุคคลที่เกี่ยวข้องกับองค์กรทั้งหมดทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตนเองรับผิดชอบซึ่งจะเป็นสิ่งสำคัญที่จะทำให้การรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรสามารถดำเนินไปได้อย่างมีประสิทธิภาพและมีประสิทธิผล

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ขั้นตอนที่ 1. <u>การตรวจสอบและการวิเคราะห์ (Identify)</u>

1.1. การบริหารและจัดการทรัพย์สิน (Asset Management)

ข้อมูล บุคลากร อุปกรณ์ ระบบและสถานที่ที่เกี่ยวข้องกับการทำงานให้บรรลุวัตถุประสงค์ตามเป้าหมาย ขององค์กรได้รับการตรวจสอบ แยกแยะ บริหารและจัดการตามความสำคัญต่อองค์กรและความเสี่ยงที่มีความเกี่ยวข้อง โดยประกอบด้วยการปฏิบัติดังนี้

1.1.1. การตรวจสอบและการทำรายการสิ่งของของอุปกรณ์และระบบภายในองค์กรทั้งหมด

1.1.2. การตรวจสอบและทำรายการสิ่งของของโปรแกรมรูปแบบต่าง ๆ เช่น Software หรือ Application เป็นต้น

1.1.3. การจัดทำแผนผังของระบบการติดต่อสื่อสารภายในองค์กรและเส้นทางการเคลื่อนไหวของข้อมูลขององค์กร

1.1.4. การตรวจสอบและการทำบัญชีรายการระบบเทคโนโลยีสารสนเทศที่นอกเหนือการควบคุมขององค์กร

1.1.5. การบริหารและการจัดลำดับความเร่งด่วนของทรัพยากร (อุปกรณ์ ข้อมูล เวลา บุคลากร และโปรแกรม) ขององค์กรให้สอดคล้องกับการจัดการชั้นความลับ ความสำคัญ และคุณค่าต่อธุรกิจขององค์กร

1.1.6. บุคลากรทั้งหมดในองค์กร รวมถึงบุคคลที่สามที่มีส่วนได้ส่วนเสียกับองค์กร มีบทบาทและหน้าที่ในการรักษาความมั่นคงปลอดภัยไซเบอร์

1.2. สภาพแวดล้อมที่เหมาะสมทางธุรกิจ (Business Environment)

การจัดลำดับความเร่งด่วนและการทำความเข้าใจใน ภารกิจ วัตถุประสงค์ ผู้ที่มีส่วนได้ส่วนเสียและกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับองค์กร ซึ่งข้อมูลดังกล่าวจะใช้ในการปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารและจัดการความเสี่ยง โดยประกอบด้วยการปฏิบัติดังนี้

1.2.1. การตรวจสอบและการสื่อสารบทบาทและหน้าที่ที่เกี่ยวข้องกับห่วงโซ่อุปทานที่สำคัญต่อการประกอบธุรกิจขององค์กร

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๖๖๖๖ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

1.2.2. การตรวจสอบและการสื่อสารบทบาทขององค์กรในส่วนที่เกี่ยวข้องกับโครงสร้างสำคัญของประเทศ หรือในภาคอุตสาหกรรมขององค์กร

1.2.3. การสร้างและการสื่อสารความเร่งด่วนของภารกิจ วัตถุประสงค์ และกิจกรรมขององค์กร

1.2.4. การตรวจสอบและการยืนยันระบบการทำงานที่สำคัญและสิ่งที่จำเป็นต่อระบบการทำงานดังกล่าว

1.2.5. การตรวจสอบและการยืนยันความต้องการของระบบการทำงานที่สำคัญขององค์กรเพื่อให้ระบบสามารถดำเนินการและปฏิบัติได้ทุกสถานภาพ เช่น ระหว่างการถูกโจมตี ระหว่างการฟื้นฟู หรือระหว่างสถานภาพปกติ เป็นต้น

1.3. การอภิบาลองค์กร (Governance)

การทำความเข้าใจในนโยบายแผนการปฏิบัติงานและกระบวนการทำงานขององค์กรในการบริหารจัดการองค์กรเพื่อให้เป็นไปตามกฎระเบียบ กฎหมาย มาตรฐานสากล ความเสี่ยงและความต้องการในทางปฏิบัติ รวมถึงการกำหนดนโยบาย แผนการปฏิบัติงานและกระบวนการทำงานขององค์กรให้เป็นไปตามการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประกอบด้วยการปฏิบัติ ดังนี้

1.3.1. การสร้างและการสื่อสารนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

1.3.2. การประสานงานและการจัดการบทบาทและความรับผิดชอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรภายในองค์กรและบุคคลภายนอกที่มีความเกี่ยวข้องกับองค์กร

1.3.3. การทำความเข้าใจและการบริหารจัดการความต้องการสำหรับกฎหมายและกฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

1.3.4. การอภิบาลองค์กรและการบริหารจัดการความเสี่ยงขององค์กร ตอบโจทย์ของความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

1.4. การวิเคราะห์ความเสี่ยง (Risk Assessment)

การทำความเข้าใจในการวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับ การปฏิบัติงานขององค์กร ทรัพย์สินในองค์กร และบุคลากรทุกคนในองค์กร โดยประกอบด้วยการปฏิบัติดังนี้

1.4.1. การประเมินความเสี่ยง ประกอบด้วย

- การระบุความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Risk Identification) ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก
- การวิเคราะห์ความเสี่ยง (Risk Analysis) เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

- การประเมินค่าความเสี่ยง (Risk Evaluation) โดยประเมินถึงโอกาสที่ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น

1.4.2. การจัดการความเสี่ยง โดยบริษัทต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

1.4.3. การติดตามและทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

1.4.4. การรายงานความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของบริษัทหรือผู้ที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมคณะกรรมการ เป็นต้น

1.5. ยุทธศาสตร์การบริหารและจัดการความเสี่ยง (Risk Management Strategy)

การจัดความเร่งด่วนของทรัพยากร ข้อจำกัด เกณฑ์ยอมรับความเสี่ยง และข้อสันนิษฐานที่เกี่ยวข้องกับการรักษาความมั่นปลอดภัยไซเบอร์ขององค์กร ถูกนำไปใช้ในการบริหารและจัดการความเสี่ยง โดยประกอบด้วยการปฏิบัติดังนี้

1.5.1. กระบวนการบริหารและจัดการความเสี่ยงขององค์กรได้รับการตรวจสอบและเป็นที่ยอมรับจากบุคคลที่เกี่ยวข้องกับการบริหารองค์กร รวมถึงผู้ที่มีส่วนได้ส่วนเสียกับองค์กร

1.5.2. การพิจารณาเกณฑ์ยอมรับความเสี่ยงขององค์กรและการเปิดเผยข้อมูลอย่างชัดเจน

1.5.3. การตรวจสอบเกณฑ์ยอมรับความเสี่ยงขององค์กรโดยภาคส่วนที่เกี่ยวข้องกับองค์กรในด้านโครงสร้างสำคัญของประเทศหรือในภาคอุตสาหกรรมที่เกี่ยวข้องกับองค์กร

1.5.4. ความเสี่ยงที่อยู่ในระดับสูงและสูงมาก ต้องมีการกำหนดตัวชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้ติดตามและทบทวนความเสี่ยง โดยกำหนดเกณฑ์ในการวัดผลมาอ้างอิงตามมาตรการควบคุมและขั้นตอนปฏิบัติงานที่นำมาใช้ในการจัดการความเสี่ยง

1.6. การบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทาน (Supply Chain Risk Management)

การจัดความเร่งด่วนของทรัพยากร ข้อจำกัด เกณฑ์ยอมรับความเสี่ยงและข้อสันนิษฐานที่เกี่ยวข้องกับการรักษาความมั่นปลอดภัยไซเบอร์ขององค์กรถูกนำไปใช้ในการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานขององค์กร โดยประกอบด้วยการปฏิบัติดังนี้

1.6.1. กระบวนการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานขององค์กร ได้รับการตรวจสอบและเป็นที่ยอมรับจากบุคคลที่เกี่ยวข้องกับการบริหารองค์กร รวมถึงผู้ที่มีส่วนได้ส่วนเสียกับองค์กร

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

1.6.2. การตรวจสอบการจัดลำดับความเร่งด่วนของทรัพยากร และการวิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการ ผู้ผลิต และบุคคลที่สามที่มีความเกี่ยวข้องกับองค์กรของระบบสารสนเทศชิ้นส่วนอุปกรณ์และบริการ

1.6.3. สัญญาที่ทำไว้กับผู้ให้บริการ ผู้ผลิต และบุคคลที่สามที่มีความเกี่ยวข้องกับองค์กรมีการตอบสนองต่อวัตถุประสงค์ขององค์กรในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการบริหารและจัดการความเสี่ยงที่เกี่ยวข้องกับห่วงโซ่อุปทานขององค์กร

1.6.4. ผู้ให้บริการ ผู้ผลิต และบุคคลที่สามที่มีความเกี่ยวข้องกับองค์กรได้รับการตรวจสอบจากบุคคลภายนอกเพื่อให้สามารถยืนยันได้ว่าบุคคลดังกล่าวได้ปฏิบัติตามสัญญาในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

1.6.5. การทดสอบแผนเผชิญเหตุและแผนฟื้นฟู ร่วมกับผู้ให้บริการ ผู้ผลิต และบุคคลที่สามที่มีความเกี่ยวข้องกับองค์กร

ขั้นตอนที่ 2. <u>การป้องกันองค์กร (Protect)</u>

2.1. การบริหารและจัดการอัตลักษณ์ของบุคลากรและการควบคุมการเข้าถึงภายในองค์กร (Identity Management and Access Control)

การจำกัดการเข้าถึงทั้งทางด้านกายภาพและด้านตรรกะต่อทรัพย์สินและสถานที่ขององค์กรให้เฉพาะผู้ที่ได้รับอนุญาต กระบวนงานที่ได้รับอนุญาตให้ปฏิบัติงาน และอุปกรณ์ที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น และการเข้าถึงดังกล่าวได้รับการบริหารจัดการโดยมีการคำนึงถึงความเสี่ยงที่มาพร้อมกับการเข้าถึงที่ไม่ได้รับอนุญาต โดยประกอบด้วยการปฏิบัติดังนี้

2.1.1. การบริหารจัดการ ยืนยัน ยกเลิกและการตรวจสอบอัตลักษณ์รวมถึงบัญชีการเข้าใช้งานของบุคลากรในองค์กรสำหรับอุปกรณ์ ผู้ใช้งานรวมถึงกระบวนงานที่ได้รับอนุญาต

2.1.2. การบริหารจัดการและการป้องกันการเข้าถึงทางกายภาพของทรัพย์สินภายในองค์กร

2.1.3. การบริหารจัดการของการปฏิบัติงานและการเข้าถึงระยะไกล

2.1.4. การบริหารจัดการสิทธิและการอนุญาตการเข้าถึง โดยคำนึงถึงหลักของการเข้าถึงเท่าที่มีความจำเป็นต่อการปฏิบัติงานและการแบ่งแยกการเข้าถึงตามหน้าที่ที่ได้รับมอบหมาย

2.1.5. การป้องกันเครือข่ายด้วยการแบ่งแยกเครือข่ายตามความสำคัญหรือแบ่งแยกตามการปฏิบัติงาน

2.1.6. การยืนยันตัวตนของผู้ใช้งาน อุปกรณ์และทรัพย์สินอื่น ๆ เพื่อเป็นการตอบสนองต่อความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

2.2. การฝึกและการให้ความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร (Awareness and Training)

บุคลากรขององค์กรได้รับการอบรมเพิ่มพูนความตระหนักรู้ถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ และได้รับการฝึกในหน้าที่และความรับผิดชอบในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประกอบด้วยการปฏิบัติดังนี้

2.2.1. บุคลากรภายในองค์กรทุกคนได้รับการอบรมและการฝึก

2.2.2. ผู้ใช้งานที่มีสิทธิการเข้าถึงพิเศษต้องเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตนเองที่มีต่อองค์กร

2.2.3. บุคคลที่สามที่มีความเกี่ยวข้องกับองค์กรมีความเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตนเองที่มีต่อองค์กร

2.2.4. ผู้บริหารระดับสูงมีความเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตนเอง

2.2.5. บุคลากรที่ทำหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์และรักษาความปลอดภัยโดยทั่วไปมีความเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตนเอง

2.3. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

การบริหารจัดการข้อมูลขององค์กรให้เป็นไปตามการวิเคราะห์ความเสี่ยงและพื้นฐานของการรักษาความมั่นคงปลอดภัยไซเบอร์ 3 ข้อ คือ การรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล และความพร้อมใช้งานของข้อมูล โดยประกอบด้วยการปฏิบัติดังนี้

2.3.1. การรักษาความปลอดภัยข้อมูลที่ได้จัดเก็บไว้

2.3.2. การรักษาความปลอดภัยข้อมูลระหว่างการโอนย้าย

2.3.3. การบริหารจัดการทรัพย์สินขององค์กรด้วยการจำหน่าย ทำลาย และการขนย้าย

2.3.4. การดำรงไว้ซึ่งความพร้อมใช้งานของข้อมูล

2.3.5. การมีระบบป้องกันข้อมูลรั่วไหล

2.3.6. การใช้ระบบการตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล เพื่อใช้ในการยืนยันโปรแกรมหรือข้อมูลที่เข้าหรือออกจากองค์กร

2.3.7. การใช้ระบบการตรวจสอบความถูกต้องสมบูรณ์ของอุปกรณ์ เพื่อใช้ในการยืนยันการทำงานอุปกรณ์ในองค์กร

2.4. การรักษาความปลอดภัยของข้อมูลในกระบวนการทำงาน (Information Protection Processes and Procedures)

การบริหารจัดการนโยบายและกระบวนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้ในการป้องกับทรัพย์สินและระบบขององค์กร โดยประกอบด้วยการปฏิบัติดังนี้

2.4.1. การตั้งค่าของการรักษาความปลอดภัยนั้นคำนึงถึงหลักสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

2.4.2. การปรับใช้วัฏจักรของระบบภายในองค์กร

2.4.3. การประยุกต์ใช้ระบบการควบคุมการตั้งค่าต่าง ๆ ภายในองค์กร

2.4.4. การเก็บรักษาและการตรวจสอบข้อมูลสำรองให้พร้อมใช้งานได้ตลอดเวลา

2.4.5. นโยบายและกฎระเบียบขององค์กรที่เกี่ยวข้องกับการรักษาความปลอดภัยขององค์กร และทรัพย์สินมีความเหมาะสม

2.4.6. การทำลายข้อมูลที่ไม่ได้ใช้งานแล้ว ตามวัฏจักรของข้อมูลที่เหมาะสม

2.4.7. การพัฒนาระบบการรักษาความปลอดภัย

2.4.8. การใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยขององค์กร

2.4.9. การบริหารจัดการและการปรับใช้แผนเผชิญเหตุ แผนความต่อเนื่องทางธุรกิจขององค์กรรวมถึงแผนการฟื้นฟูองค์กรจากภัยต่าง ๆ

2.4.10. การตรวจสอบแผนเผชิญเหตุ แผนความต่อเนื่องทางธุรกิจขององค์กร และแผนการฟื้นฟูองค์กรจากภัยต่าง ๆ ตามเวลา

2.4.11. ฝ่ายทรัพยากรบุคคลประยุกต์ใช้หลักของการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การตรวจสอบพื้นหลังของบุคคล เป็นต้น

2.4.12. การพัฒนาและการปรับใช้แผนการบริหารและจัดการช่องโหว่ขององค์กร

2.5. การบำรุงรักษา (Maintenance)

การบำรุงรักษาและการซ่อมแซมอุปกรณ์ควบคุม รวมถึงอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศตามเวลาที่สอดคล้องนโยบายและแผนการปฏิบัติงานขององค์กร โดยประกอบด้วยการปฏิบัติดังนี้

2.5.1. การบำรุงรักษาและการซ่อมแซมอุปกรณ์ โดยเครื่องมือที่ได้รับการตรวจสอบ ควบคุมและอนุญาตเท่านั้น โดยต้องมีการบันทึกการปฏิบัติทุกครั้ง

2.5.2. สำหรับการบำรุงรักษาหรือการซ่อมแซมอุปกรณ์ ที่เป็นการปฏิบัติผ่านโปรแกรมช่วยเหลือจากระยะไกล ต้องได้รับการอนุญาตและบันทึกการปฏิบัติเสมอ โดยในระหว่างการปฏิบัติงานนั้นต้องมีมาตรการป้องกันการเข้าถึงที่ไม่รับอนุญาต

2.6. เทคโนโลยีที่ช่วยในการป้องกันและรักษาความปลอดภัยองค์กร (Protective Technology)

การใช้บริการเทคโนโลยีที่มีอยู่เพื่อเพิ่มความทนทานและความยืดหยุ่นในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรให้เป็นไปตามแนวคิดของการออกแบบระบบการรักษาความมั่นคงปลอดภัยไซเบอร์แบบหลายชั้น (Defense in depth) และให้สอดคล้องกับนโยบายรวมถึงแนวปฏิบัติในการรักษาความปลอดภัยขององค์กร โดยประกอบด้วยการปฏิบัติดังนี้

2.6.1. การกำหนด จัดเก็บ ใช้งานและตรวจสอบข้อมูลการตรวจสอบจากบุคคลภายนอกและข้อมูลบันทึกเหตุการณ์ในองค์กร ให้เป็นไปตามนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

2.6.2. การควบคุม ป้องกัน และจำกัดการใช้งานอุปกรณ์ที่สามารถถอดออกหรือเคลื่อนย้ายได้

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

2.6.3. การใช้หลักการกำหนดสิทธิการเข้าถึงหรือการเข้าใช้งานระบบเครือข่ายข้อมูล หรือบริการสารสนเทศที่องค์กรมีทั้งหมดให้อย่างน้อยเป็นไปตามความจำเป็นเท่าที่ผู้ที่ได้รับอนุญาตสามารถทำงานได้ (Least privilege basis) และให้อย่างน้อยเป็นไปตามความต้องการพื้นฐานสำหรับการทำงานตามที่ได้รับอนุญาตเท่านั้น (Need to know basis)

2.6.4. การป้องกันระบบการติดต่อสื่อสารและระบบการควบคุมองค์กรบนเครือข่ายขององค์กรตามหลักการรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล และความพร้อมใช้งาน (CIA)

2.6.5. การใช้เทคโนโลยีที่เกี่ยวข้องกับระบบการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเพิ่มความยืดหยุ่น ในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับองค์กรทั้งในยามปกติและยามคับขัน เช่น อุปกรณ์ป้องกันภัยจากความผิดพลาด (Failsafe system) หรือระบบกระจายการทำงานของเครื่องแม่ข่าย (Load balancer) เป็นต้น

2.7. แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร ต้องมีการสื่อสารไปยังบุคลากรที่เกี่ยวข้องทั้งหมด และต้องทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ 1 ครั้ง โดยนับตั้งแต่วันที่แผนได้รับอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์

ขั้นตอนที่ 3. <u>การตรวจจับเหตุการณ์ทั้งหมดขององค์กร (Detect)</u>

3.1. เหตุการณ์โดยทั่วไปและเหตุกรณ์ที่ผิดปกติ (Anomalies and Events)

การตรวจจับเหตุการณ์ที่ผิดปกติและการทำความเข้าใจถึงผลกระทบที่อาจจะเกิดขึ้นของเหตุการณ์ที่ผิดปกตินั้นได้ โดยประกอบด้วยการปฏิบัติดังนี้

3.1.1. การจัดตั้งและควบคุมระบบการปฏิบัติงานบนเครือข่ายและเส้นทางการไหลของข้อมูลของผู้ใช้งาน

3.1.2. การตรวจจับและการวิเคราะห์เหตุการณ์เพื่อทำความเข้าใจถึงเป้าหมายของการโจมตีและวิธีการที่ใช้โจมตี

3.1.3. การเก็บข้อมูลของเหตุการณ์และการตรวจสอบความเชื่อมโยงของข้อมูลเหตุการณ์ทั้งหมด

3.1.4. การพิจารณาผลกระทบของเหตุการณ์ที่อาจจะเกิดขึ้น

3.1.5. การวางระบบการแจ้งเตือนเหตุการณ์ที่เหมาะสม

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

3.2. การเฝ้าระวังการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง (Security Continuous Monitoring)

การเฝ้าระวังระบบสารสนเทศและทรัพย์สินเพื่อแยกแยะเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ และการตรวจสอบประสิทธิภาพของมาตรการที่ใช้ในการรักษาความปลอดภัย โดยประกอบด้วยการปฏิบัติดังนี้

3.2.1. การตรวจสอบเครือข่ายขององค์กรเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2.2. การตรวจสอบสภาพแวดล้อมและการป้องกันทางกายภาพ เพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2.3. การตรวจสอบกิจกรรมของบุคลากรในองค์กร เพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2.4. การตรวจจับโค้ดโปรแกรมประสงค์ร้าย

3.2.5. การตรวจจับโค้ดโปรแกรมที่ไม่ได้รับอนุญาต

3.2.6. การตรวจสอบกิจกรรมของผู้ให้บริการภายนอกองค์กรเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2.7. การตรวจสอบบุคลากรที่ไม่ได้รับอนุญาต การเชื่อมต่อกับเครือข่ายที่ไม่ได้รับอนุญาต อุปกรณ์ที่ไม่ได้รับอนุญาต และโปรแกรมที่ไม่ได้รับอนุญาตภายในองค์กร

3.2.8. การตรวจสอบช่องโหว่ภายในองค์กร

3.3. กระบวนการตรวจจับ (Detection Processes)

การทดสอบและดำรงไว้ซึ่งกระบวนการตรวจจับเหตุการณ์ที่ผิดปกติเพื่อให้องค์กรมีความตระหนักถึงภัยคุกคามที่มาพร้อมกับเหตุการณ์ที่ผิดปกติ โดยประกอบด้วยการปฏิบัติดังนี้

3.3.1. การแบ่งมอบหน้าที่และความรับผิดชอบในการตรวจจับเหตุการณ์ที่ผิดปกติโดยชัดเจน

3.3.2. การตรวจสอบเป็นไปตามความต้องการของกฎหมาย ระเบียบ หรือมาตรฐานสากล

3.3.3. การทดสอบกระบวนการตรวจจับเหตุการณ์ที่ผิดปกติ

3.3.4. การติดต่อสื่อสารข้อมูลที่ได้จากการตรวจจับเหตุการณ์ที่ผิดปกติไปยังส่วนที่เกี่ยวข้องภายในองค์กร

3.3.5. การพัฒนากระบวนการตรวจจับเหตุการณ์ที่ผิดปกติอย่างต่อเนื่อง

3.4. ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง โดยมีขอบเขตการตรวจสอบ ดังนี้

3.4.1.กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

3.4.2.บริการที่สำคัญที่บริษัทเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ 3.4.1

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

ขั้นตอนที่ 4. <u>การตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (Respond)</u>

4.1. การวางแผนเผชิญเหตุ (Response Planning)

การปฏิบัติและดำรงไว้ซึ่งกระบวนการและแผนการปฏิบัติการในการเผชิญเหตุเพื่อให้องค์กรสามารถตอบสนองต่อเหตุที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตรวจจับได้อย่างเหมาะสม โดยประกอบด้วยการปฏิบัติดังนี้

4.1.1. การใช้แผนเผชิญเหตุในระหว่างการเกิดเหตุการณ์และหลังจากการเกิดเหตุการณ์

4.2. การประสานงานและการติดต่อสื่อสาร (Communications)

ประสานงานที่เกี่ยวข้องกับแผนเผชิญเหตุกับบุคลากรทั้งหมดในองค์กร และบุคคลหรือองค์กรภายนอกที่มีส่วนได้ส่วนเสียกับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (เช่น หน่วยงาน ราชการ หน่วยงานทางกฎหมาย เป็นต้น) โดยประกอบด้วยการปฏิบัติดังนี้

4.2.1. บุคลากรในองค์กรทราบและเข้าใจในการปฏิบัติเมื่อเริ่มใช้แผนเผชิญเหตุ

4.2.2. รายงานเหตุการณ์ที่เกิดขึ้นกับหน่วยงานที่เกี่ยวข้อง

4.2.3. สื่อสารข้อมูลที่เกี่ยวข้องกับเหตุทางไซเบอร์ให้กับบุคลากรพร้อมกับแนวทางการใช้แผนเผชิญเหตุที่เหมาะสม

4.2.4. ประสานการปฏิบัติกับบุคคลหรือองค์กรภายนอกที่มีส่วนได้ส่วนเสียกับเหตุการณ์ที่เกี่ยวข้องกับเหตุทางไซเบอร์พร้อมกับแนวทางการใช้แผนเผชิญเหตุที่เหมาะสม

4.2.5. การแบ่งปันข้อมูลข่าวสารที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับบุคคลหรือองค์กรภายนอกที่มีส่วนได้ส่วนเสียกับองค์กร เพื่อให้ภาคส่วนหรือประชาคมมีความตระหนักรู้และเข้าใจการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ดียิ่งขึ้น

4.3. การวิเคราะห์เหตุการณ์ที่เกิดขึ้น (Analysis)

วิเคราะห์เหตุการณ์ที่เกิดขึ้นเพื่อให้สามารถใช้แผนเผชิญเหตุและแผนการฟื้นฟูองค์กรได้อย่างมีประสิทธิภาพ โดยประกอบด้วยการปฏิบัติดังนี้

4.3.1. การตรวจสอบระบบการแจ้งเตือนจากระบบการตรวจจับเหตุการณ์ที่ผิดปกติที่เกิดขึ้นกับองค์กร

4.3.2. ทำความเข้าใจผลกระทบของเหตุการณ์ที่เกิดขึ้น

4.3.3. การเก็บหลักฐานทางดิจิทัล

4.3.4. การพิสูจน์หลักฐานทางดิจิทัล

4.3.5. แบ่งแยกเหตุการณ์ที่เกิดขึ้นตามความเหมาะสมกับแผนเผชิญเหตุที่ได้จัดเตรียมไว้

4.3.6. มีกระบวนการที่ใช้ในการตรวจสอบ วิเคราะห์ และตอบสนองต่อช่องโหว่ที่ได้รับการเปิดเผย ทั้งจากภายในและภายนอกองค์กร เช่น การตรวจสอบช่องโหว่ขององค์กร บทความที่เกี่ยวข้องกับช่องโหว่ที่ได้รับการตรวจสอบและเผยแพร่โดยทั่วไป หรือการค้นคว้าโดยเจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์

เลขที่ ๑๒๐ อาคารธนพิทัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๗๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

4.4. การปฏิบัติเพื่อป้องกันหรือลดโอกาสของเหตุการณ์ที่ไม่ปกติ (Mitigation)

มีการปฏิบัติการเพื่อเป็นการป้องกันหรือลดโอกาสที่เหตุการณ์ผิดปกติจะเกิดขึ้น รวมถึงลดผลกระทบหรือช่วยในการคลี่คลายเหตุการณ์ที่ไม่ปกติ โดยประกอบด้วยการปฏิบัติดังนี้

4.4.1. การจำกัดวงของเหตุการณ์ผิดปกติหรือภัยที่เกิดขึ้น

4.4.2. การป้องกันและการลดโอกาสในการเกิดเหตุการณ์ผิดปกติหรือภัยที่เกิดขึ้น

4.4.3. การตรวจสอบ การบันทึก การป้องกันและการลดโอกาสของความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์จากช่องโหว่ใหม่ที่ตรวจพบ

4.5. การพัฒนา (Improvements)

พัฒนาความสามารถในการตอบโต้ภัยคุกคามทางไซเบอร์ โดยการใช้เหตุการณ์ที่เคยเกิดขึ้นกับองค์กรเป็นบทเรียนในการพัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยประกอบด้วยการปฏิบัติดังนี้

4.5.1. การทำแผนเผชิญเหตุเป็นการประยุกต์จากบทเรียนจากเหตุการณ์ที่เกิดขึ้นกับองค์กร

4.5.2. ยุทธศาสตร์ในการตอบโต้เหตุการณ์มีการปรับปรุงให้ทันสมัยอยู่ตลอดเวลา

ขั้นตอนที่ 5. <u>การฟื้นฟูองค์กร (Recovery)</u>

5.1. แผนในการฟื้นฟูองค์กร (Recovery Planning)

การปฏิบัติและดำรงไว้ซึ่งกระบวนการในการฟื้นฟูองค์กรเพื่อทำให้มั่นใจได้ว่าระบบและทรัพย์สินขององค์กรได้รับการฟื้นฟูหลังจากผลกระทบจากภัยคุกคามทางไซเบอร์ โดยประกอบด้วยการปฏิบัติดังนี้

5.1.1. การใช้แผนการฟื้นฟูองค์กรในระหว่างการเกิดเหตุการณ์และหลังจากการเกิดเหตุการณ์

5.2. การพัฒนา (Improvements)

องค์กรพัฒนาแผนการฟื้นฟูองค์กรจากภัยคุกคามทางไซเบอร์ด้วยการใช้เหตุการณ์ที่เคยเกิดขึ้นกับองค์กรเป็นบทเรียนในการพัฒนาขั้นตอนและระบบในการฟื้นฟูองค์กร โดยประกอบด้วยการปฏิบัติดังนี้

5.2.1. การทำแผนการฟื้นฟูองค์กรเป็นการประยุกต์จากบทเรียนจากเหตุการณ์ที่เกิดขึ้นกับองค์กร

5.2.2. ยุทธศาสตร์ในการฟื้นฟูองค์กรมีปรับปรุงให้ทันสมัยอยู่ตลอดเวลา

5.3. การประสานงานและการติดต่อสื่อสาร (Communications)

5.4. องค์กรประสานงานที่เกี่ยวข้องกับแผนการฟื้นฟูองค์กรกับบุคลากรทั้งหมดในองค์กรและบุคคลหรือองค์กรภายนอกที่มีส่วนได้ส่วนเสียกับเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (เช่น หน่วยงานราชการ หน่วยงานทางกฎหมาย ผู้ให้บริการภายนอก เจ้าของระบบที่โจมตีจากภัยคุกคามทางไซเบอร์ ผู้ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ เป็นต้น) โดยประกอบด้วยการปฏิบัติดังนี้

5.4.1. การบริหารจัดการกิจการที่เกี่ยวข้องกับการประชาสัมพันธ์

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๙๙๙๙ www.dad.co.th

5.4.2. การฟื้นฟูชื่อเสียงและภาพพจน์ขององค์กรหลังจากที่เกิดเหตุการณ์ที่ไม่ปกติหรือภัยคุกคามทางไซเบอร์

5.4.3. องค์กรมีการประสานงานและติดต่อสื่อสารกิจกรรมที่เกี่ยวข้องกับการฟื้นฟูองค์กรกับบุคลากรทั้งหมดในองค์กร ผู้มีส่วนได้ส่วนเสียกับองค์กรภายนอก และคณะผู้บริหารขององค์กร

7. ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
3) NIST Cybersecurity Framework
4) ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 (บังคับใช้วันที่ 6 กันยายน พ.ศ. 2564)
5) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (บังคับใช้วันที่ 18 มกราคม พ.ศ. 2567)
6) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 (บังคับใช้วันที่ 18 มกราคม พ.ศ. 2567)
7) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (บังคับใช้วันที่ 3 กันยายน พ.ศ. 2567)

8. การทบทวนนโยบายข้อมูล

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด คณะกรรมการ ผู้บริหาร และหน่วยงานรับผิดชอบต้องร่วมกันดำเนินการทบทวนนโยบาย เมื่อมีการเปลี่ยนแปลงที่สำคัญหรือตามความเหมาะสม และจัดให้มีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง

ประกาศ ณ วันที่ 24 พฤศจิกายน 2568

(นายนาฬิกอติภัค แสงสนิท)

กรรมการผู้จัดการ

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th