ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด
เรื่อง แนวปฏิบัติการใช้อุปกรณ์ Internet of Things (IoT) อย่างปลอดภัย

---

1. วัตถุประสงค์

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) ตระหนักถึงความสำคัญของการใช้อุปกรณ์ Internet of Things (IoT) ในการยกระดับประสิทธิภาพการดำเนินงานและการให้บริการ อุปกรณ์ IoT เช่น กล้องวงจรปิดอัจฉริยะ เซ็นเซอร์ตรวจวัดสภาพแวดล้อม และอุปกรณ์สวมใส่ (Wearable Devices) มีความสามารถในการเก็บ ประมวลผล และส่งต่อข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเพิ่มความสะดวกและศักยภาพในการทำงาน แต่ก็มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การรั่วไหลของข้อมูล และการถูกโจมตีผ่านช่องโหว่ของระบบ ดังนั้น แนวปฏิบัตินี้จึงถูกจัดทำขึ้นเพื่อกำหนดหลักเกณฑ์และขั้นตอนในการใช้อุปกรณ์ IoT ภายใน ธพส. ให้มีความปลอดภัย สอดคล้องกับกฎหมาย มาตรฐานสากล และแนวทางความมั่นคงปลอดภัยไซเบอร์ภาครัฐ เพื่อลดความเสี่ยงจากการโจมตี ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล

2. ขอบเขตและการบังคับใช้

ขอบเขตของแนวปฏิบัตินี้ครอบคลุมการใช้อุปกรณ์ IoT ทั้งที่เป็นทรัพย์สินของ ธพส. และที่นำมาใช้เชื่อมต่อกับระบบงานขององค์กร ไม่ว่าจะใช้งานภายในอาคารสำนักงาน พื้นที่โครงการ หรือพื้นที่ปฏิบัติงานภายนอกผู้ที่อยู่ในขอบเขตการบังคับใช้ ได้แก่ คณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และผู้รับจ้างภายนอกของ ธพส. ที่มีสิทธิ์เข้าถึงหรือใช้งานอุปกรณ์ IoT ในนามองค์กร

3. ข้อยกเว้น

การใช้อุปกรณ์ IoT เพื่อวัตถุประสงค์ส่วนบุคคลที่ไม่เกี่ยวข้องกับงานของ ธพส. จะไม่อยู่ภายใต้แนวปฏิบัตินี้ เว้นแต่มีการเชื่อมต่อกับระบบเครือข่ายหรือฐานข้อมูลขององค์กร ซึ่งต้องได้รับอนุญาตจากฝ่ายดิจิทัล และต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยที่เกี่ยวข้อง

4. บทบาทและความรับผิดชอบ

บทบาทและความรับผิดชอบกำหนดตามตารางต่อไปนี้

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	• ทำหน้าที่พิจารณากลั่นกรอง กำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีดิจิทัล

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

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
กรรมการผู้จัดการ	กรรมการผู้จัดการ	• กำหนดและส่งเสริมให้การใช้อุปกรณ์ IoT เป็นไปตามแนวปฏิบัติสนับสนุนทรัพยากรและงบประมาณ
ผู้บริหาร	รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ ผู้อำนวยการฝ่ายที่เกี่ยวข้อง หรือพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วนหรือผู้ชำนาญการขึ้นไป	• ประเมินความเสี่ยง จัดทำแผนการใช้อุปกรณ์ IoT สื่อสารและกำกับดูแลในหน่วยงาน
พนักงาน	พนักงานทุกคนภายใน ธพส.	• ปฏิบัติตามแนวปฏิบัติ รักษาความปลอดภัยของอุปกรณ์ และรายงานเหตุผิดปกติ
หน่วยงานรับผิดชอบ	ฝ่ายดิจิทัล	• จัดหาและติดตั้งอุปกรณ์ IoT อย่างปลอดภัย กำหนดมาตรการความปลอดภัย เฝ้าระวัง และบันทึกการใช้งาน

5. คำนิยาม

"บริษัท" หมายถึง บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด หรือ เรียกโดยย่อว่า ธพส.

"คณะกรรมการ" หมายถึง คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล

"กรรมการผู้จัดการ" หมายถึง กรรมการผู้จัดการของ ธพส.

"ผู้บริหาร" หมายถึง กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ ผู้อำนวยการฝ่ายที่เกี่ยวข้อง และพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วน หรือผู้ชำนาญการขึ้นไป

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

"หน่วยงานรับผิดชอบ" หมายถึง คณะทำงาน คณะกรรมการ ฝ่ายงานของ ธพส. ที่รับผิดชอบในการพัฒนาระบบบริหารจัดการ และระบบบเทคโนโลยีดิจิทัลเพื่อสนับสนุนการดำเนินงานตามนโยบาย

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

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

"อุปกรณ์ IoT (Internet of Things Devices)" หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่มีความสามารถในการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อเก็บ ประมวลผล และแลกเปลี่ยนข้อมูล เช่น กล้องวงจรปิดอัจฉริยะ อุปกรณ์สมาร์ทโฮม เซ็นเซอร์ตรวจวัด และอุปกรณ์สวมใส่

"ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)" หมายถึง การปกป้องระบบเครือข่าย อุปกรณ์ และข้อมูลจากการโจมตี การเข้าถึงโดยไม่ได้รับอนุญาต หรือการรั่วไหลของข้อมูล

"รหัสผ่านตั้งต้น (Default Password)" หมายถึง รหัสผ่านที่ถูกตั้งมาโดยผู้ผลิตและมักเหมือนกันในอุปกรณ์รุ่นเดียวกัน

"รหัสผ่าน (Password)" หมายถึง ตัวอักษร หรืออักขระพิเศษ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัว บุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

"Least Privilege" หมายถึง หลักการกำหนดสิทธิ์การเข้าถึงระบบหรือข้อมูล โดยให้สิทธิ์แก่ผู้ใช้ โปรแกรม หรือกระบวนการ เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น เพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้สิทธิ์เกินความจำเป็น และจำกัดผลกระทบหากเกิดเหตุด้านความมั่นคงปลอดภัยขึ้น

6. หลักการและแนวปฏิบัติ

1) การตั้งค่าความปลอดภัยขั้นต้น

1.1) อุปกรณ์ IoT ทุกชิ้นต้องผ่านการตรวจสอบและอนุมัติจากฝ่ายดิจิทัลก่อนนำมาใช้งานในเครือข่ายของบริษัท

1.2) ต้องเปลี่ยนรหัสผ่านตั้งต้น (Default Password) ทันทีหลังติดตั้ง ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข เข้าด้วยกัน (อ้างอิงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ส่วนที่ 1 นโยบายการเข้าถึงและการใช้งานสารสนเทศ เรื่องที่ 5 การบริหารจัดการ และการใช้งานรหัสผ่าน)

1.3) ปิดบริการหรือฟังก์ชันที่ไม่จำเป็นต่อการใช้งาน เช่น Remote Access, Location Services หรือการเข้าถึงจากระยะไกลอื่น ๆ เพื่อลดพื้นที่การโจมตี (Attack Surface)

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

1.4) กำหนดสิทธิ์การเข้าถึง (Access Control) ตามหลักการ “Least Privilege” โดยอนุญาตให้เฉพาะผู้ที่มีความจำเป็นต่อการปฏิบัติงาน

2) การเชื่อมต่อเครือข่าย

2.1) อุปกรณ์ IoT ต้องเชื่อมต่อผ่านเครือข่ายที่แยกส่วน (Network Segmentation) จากเครือข่ายหลักขององค์กร เพื่อจำกัดผลกระทบในกรณีที่เกิดการบุกรุก

2.2) ใช้เฉพาะเครือข่ายที่ได้รับการรับรองจากฝ่ายดิจิทัล หรือ Virtual Private Network (VPN) ที่มีการเข้ารหัสข้อมูล

2.3) หลีกเลี่ยงการเชื่อมต่อกับเครือข่ายสาธารณะหรือเครือข่ายที่ไม่ผ่านการตรวจสอบ

2.4) ฝ่ายดิจิทัลต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) บนเครือข่าย IoT

3) การอัปเดตและบำรุงรักษา

3.1) อัปเดตเฟิร์มแวร์และซอฟต์แวร์ของอุปกรณ์ IoT อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ด้านความปลอดภัย โดยใช้เฉพาะไฟล์อัปเดตจากผู้ผลิตที่เชื่อถือได้

3.2) จัดทำแผนและตารางบำรุงรักษาอุปกรณ์ พร้อมบันทึกประวัติการบำรุงรักษาและแจ้งให้กับฝ่ายดิจิทัลรับทราบ

3.3) ตรวจสอบการทำงานของอุปกรณ์อย่างน้อยไตรมาสละ 1 ครั้ง เพื่อค้นหาความผิดปกติหรือพฤติกรรมที่บ่งชี้ถึงการโจมตี

4) การปกป้องข้อมูล

4.1) ข้อมูลที่ส่งระหว่างอุปกรณ์และระบบต้องถูกเข้ารหัส (Encryption in Transit) โดยใช้โปรโตคอลความปลอดภัยมาตรฐาน เช่น TLS 1.3

4.2) ข้อมูลที่จัดเก็บในอุปกรณ์ต้องมีการเข้ารหัส (Encryption at Rest) และมีการควบคุมสิทธิ์การเข้าถึง

4.3) ห้ามบันทึกข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กรลงในอุปกรณ์ IoT เว้นแต่มีมาตรการคุ้มครองที่เพียงพอและได้รับการอนุมัติเป็นลายลักษณ์อักษรจากฝ่ายดิจิทัล

5) การตรวจสอบและติดตาม

5.1) อุปกรณ์ IoT ต้องติดตั้งระบบบันทึกการใช้งาน (Logging) และระบบติดตาม (Monitoring) ที่สามารถแจ้งเตือนเหตุผิดปกติได้

5.2) ตรวจสอบ Log อย่างน้อยไตรมาสละ 1 ครั้ง และเมื่อมีเหตุการณ์ผิดปกติ ต้องวิเคราะห์และรายงานทันที

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

5.3) จัดเก็บ Log ในพื้นที่ที่มีการป้องกันและเข้าถึงได้เฉพาะบุคลากรที่ได้รับอนุญาต

6) การจัดการเหตุการณ์

6.1) หากพบอุปกรณ์ IoT สูญหาย ถูกขโมย หรือมีการใช้งานผิดปกติ ต้องรายงานต่อฝ่ายดิจิทัลเพื่อปิดการเชื่อมต่อ

6.2) ฝ่ายดิจิทัลต้องมีมาตรการป้องกันและตอบสนอง เช่น Remote Lock หรือ Remote Wipe เพื่อหยุดการเข้าถึงข้อมูล

6.3) ต้องทำการ Quarantine อุปกรณ์ที่มีความเสี่ยง และตรวจสอบสาเหตุก่อนนำกลับมาใช้งาน

7) การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

7.1) จัดฝึกอบรมบุคลากรและผู้รับจ้างเกี่ยวกับความเสี่ยงของการใช้อุปกรณ์ IoT และขั้นตอนการใช้งานอย่างปลอดภัยอย่างน้อยปีละ 1 ครั้ง

7.2) จัดทำและเผยแพร่คู่มือแนวปฏิบัติด้านความปลอดภัยของอุปกรณ์ IoT ผ่านระบบ Intranet และช่องทางสื่อสารภายในองค์กร

7.3) มีการสื่อสารเตือนภัย (Security Alert) เมื่อพบช่องโหว่หรือภัยคุกคามใหม่ที่เกี่ยวข้องกับ IoT

8) การควบคุมการนำอุปกรณ์ IoT มาใช้งาน (IoT Deployment Control)

8.1) ห้ามหน่วยงานหรือบุคลากรใดภายในบริษัท ติดตั้งหรือเชื่อมต่ออุปกรณ์ IoT เข้ากับระบบเครือข่ายขององค์กร โดยไม่ผ่านการตรวจสอบและอนุมัติจากฝ่ายดิจิทัล

8.2) ผู้รับจ้างภายนอกที่นำอุปกรณ์ IoT เข้ามาใช้ในโครงการ ต้องแจ้งรายละเอียดอุปกรณ์ต่อฝ่ายดิจิทัลเพื่อทำการตรวจสอบและอนุมัติก่อนเริ่มใช้งาน

7. ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

4) วิธีปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ภาครัฐ โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ DGA

5) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (บังคับใช้วันที่ 3 กันยายน พ.ศ. 2567)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๔๔๔๙ www.dad.co.th

6) ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 (บังคับใช้วันที่ 6 กันยายน พ.ศ. 2564)

7) ISO/IEC 27001:2022 Information Security Management System (ISMS)

8) ISO/IEC 30141:2024 Internet of Things (IoT) Reference Architecture

9) NIST Special Publication 800-183 – Networks of 'Things'

10) ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

11) ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Policy)

8. การทบทวนนโยบายข้อมูล

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด คณะกรรมการ ผู้บริหาร และหน่วยงานรับผิดชอบต้องร่วมกันดำเนินการทบทวนแนวปฏิบัติเมื่อมีการเปลี่ยนแปลงที่สำคัญหรือตามความเหมาะสม และจัดให้มีการทบทวนแนวปฏิบัติฉบับนี้อย่างน้อยปีละ 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 ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th