นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล
สำหรับศูนย์คอมพิวเตอร์และห้องมั่นคง กปภ. (ฉบับเผยแพร่)

1. วัตถุประสงค์

- เพื่อรักษาความมั่นคงปลอดภัยให้แก่ทรัพย์สินขององค์กร โดยเฉพาะอย่างยิ่งทรัพย์สินที่เป็นข้อมูลสำคัญในการดำเนินธุรกิจ โดยการปกป้องให้พ้นจากภัยคุกคามและความเสี่ยง ทั้งจากภายในและภายนอกองค์กร ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่เจตนาก็ตาม รวมถึงเพื่อลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นจากเหตุละเมิดความมั่นคงปลอดภัย และเพื่อรักษาไว้ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง

2. ขอบข่าย

- ศูนย์คอมพิวเตอร์และห้องมั่นคง อาคาร 4 ชั้น 2 สำนักงานใหญ่ การประปาส่วนภูมิภาค ซึ่งครอบคลุมเฉพาะทรัพย์สิน และระบบสารสนเทศที่ใช้ในการบริหารจัดการศูนย์คอมพิวเตอร์และห้องมั่นคง

3. คำจำกัดความ

- **องค์กร** หมายความถึง ศูนย์คอมพิวเตอร์และห้องมั่นคง สำนักงานใหญ่ การประปาส่วนภูมิภาค
- **ระบบ ISMS** หมายความถึง ระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001
- **กปภ.** หมายความถึง การประปาส่วนภูมิภาค
- **ทรัพย์สิน** (Assets) หมายความถึง สิ่งต่าง ๆ ที่มีความจำเป็นต่อการดำเนินธุรกิจภายในขอบเขตของระบบ ISMS แบ่งออกได้เป็น 5 ประเภท ได้แก่
    1. ข้อมูล (Information Asset) หมายความถึง ข้อมูลต่าง ๆ เช่น ฐานข้อมูลลูกค้า หนังสือสัญญา คู่มือปฏิบัติงาน เป็นต้น
    2. ซอฟต์แวร์ (Software Asset) หมายความถึง ซอฟต์แวร์ต่าง ๆ เช่น OS Database Development tool เป็นต้น
    3. ฮาร์ดแวร์ (Physical Asset) หมายความถึง อุปกรณ์ต่าง ๆ เช่น Server Network Equipment PC สื่อบันทึกข้อมูล เป็นต้น
    4. บุคลากร (Personnel Asset) หมายความถึง บุคลากรในตำแหน่งต่าง ๆ เช่น Developer System Administrator เป็นต้น
    5. บริการ (Service Asset) หมายความถึง บริการที่ได้รับต่าง ๆ เช่น ระบบปรับอากาศ ระบบแสงสว่าง ระบบสื่อสาร บริการซ่อมบำรุง เป็นต้น
- **พนักงาน** หมายความถึง พนักงานในสังกัดกองคอมพิวเตอร์และเครือข่าย งานศูนย์คอมพิวเตอร์ งานควบคุมระบบเครือข่าย และงานเฝ้าระวังและควบคุมความปลอดภัย

4. นโยบาย

1. ข้อมูลที่สำคัญขององค์กรต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต ต้องมีการรักษาความลับอย่างเหมาะสม ต้องมีความถูกต้อง สมบูรณ์ครบถ้วน และต้องมีความพร้อมใช้งานอยู่เสมอ
2. พนักงานทุกคนต้องปฏิบัติตามมาตรฐาน ISO 27001 และมาตรฐานอื่น ๆ ตลอดจนนโยบายด้านความมั่นคงปลอดภัยที่องค์กรกำหนด เพื่อความมั่นคงปลอดภัยของข้อมูล รวมถึงต้องปฏิบัติตามข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องทั้งหมด
3. พนักงานทุกคนต้องได้รับการฝึกอบรม และการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยของข้อมูล
4. ให้มีการบริหารจัดการความเสี่ยง (Risk management) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลในองค์กร
5. ให้มีเอกสารนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูล และเอกสารสนับสนุนที่เกี่ยวข้องเพื่อกำหนดระเบียบปฏิบัติ ตลอดจนแนวทางการปฏิบัติงาน และการใช้งานข้อมูลอย่างมั่นคงปลอดภัย
6. ให้มีการใช้งานข้อมูลระบบสารสนเทศ และทรัพย์สินขององค์กรอย่างมีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง
7. ให้มีการบริหารจัดการทรัพยากรบุคคลขององค์กรอย่างมั่นคงปลอดภัยตั้งแต่ก่อนจ้างงาน ระหว่างว่าจ้าง และหลังเลิกจ้างงาน
8. ให้มีการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและระบบสารสนเทศขององค์กรอย่างเหมาะสม
9. ให้มีข้อกำหนดการเข้าถึง การใช้งานสารสนเทศและการบริหารความมั่นคงปลอดภัยของระบบเครือข่ายเพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศขององค์กร
10. ให้มีข้อกำหนดการควบคุมการจัดซื้อ จัดจ้าง จัดพัฒนา และการบำรุงรักษาระบบสารสนเทศอย่างมั่นคงปลอดภัย
11. ให้มีกระบวนการในการบริหารจัดการกับเหตุละเมิดความมั่นคงปลอดภัยอย่างเหมาะสม และให้มีการบริหารความต่อเนื่องในการดำเนินธุรกิจ พร้อมทั้งทำการดูแลรักษา ทบทวนและทดสอบแผนอย่างน้อยปีละ 1 ครั้ง
12. กฎหมาย กฎระเบียบ นโยบายและข้อบังคับที่เกี่ยวข้องต่าง ๆ ต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วนหากผู้ใช้งาน พนักงาน ลูกจ้าง และบุคคลภายนอกฝ่าฝืนหรือก่อให้เกิดความเสียหายต่อองค์กร และ กปภ. หรือบุคคลหนึ่งบุคคลใด กปภ. จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ใช้งานที่ฝ่าฝืนตามความเหมาะสม