

**POL-IT-001**

**นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ  
(Information Security Policy)**



**บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน)**

เวอร์ชันเอกสาร:	1.0
มีผลบังคับใช้:	16 สิงหาคม พ.ศ. 2566
ผู้อนุมัติ:	คณะกรรมการบริษัท
ระดับชั้นข้อมูล:	ใช้ภายใน

## สารบัญ

	หน้า
ประวัติการปรับปรุงเอกสาร	3
รับรองเอกสาร	3
นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)	4
ขอบเขต	4
วัตถุประสงค์	4

- For www.rabbitholdings.co.th Only -

## ประวัติการปรับปรุงเอกสาร

วันที่ปรับปรุง	ปรับปรุงโดย	รายละเอียด

## รับรองเอกสาร

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
(.....) ตำแหน่ง.....	(.....) ตำแหน่ง.....	(.....) ตำแหน่ง.....
วันที่.....	วันที่.....	วันที่.....

# นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

## (Information Security Policy)

### ขอบเขต

การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับโครงสร้างพื้นฐานระบบสารสนเทศ บริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน)

### วัตถุประสงค์

เพื่อให้การดำเนินการบริหารจัดการงานด้านเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล รวมถึงข้อมูลและทรัพย์สินสารสนเทศของบริษัท แรบบิท โฮลดิ้งส์ จำกัด (มหาชน) (“บริษัทฯ”) มีการรักษาความลับอย่างเหมาะสม มีความถูกต้อง ครบถ้วน สมบูรณ์ มีความพร้อมในการดำเนินงาน และสอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ บริษัทฯ จึงเห็นควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อเป็นกรอบในการบริหารจัดการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ภายใต้ขอบเขตการขอรับรองตามมาตรฐาน ISO/IEC 27001:2022 ดังนี้

#### ข้อ 1. การตรวจสอบและประเมินความเสี่ยง

บริษัทฯ ต้องจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่ยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

#### ข้อ 2. การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

บริษัทฯ ต้องจัดให้มีกระบวนการในการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัทฯ และเพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

#### ข้อ 3. การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

บริษัทฯ ต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งาน การบำรุงรักษาด้านกายภาพและด้านสภาพแวดล้อมของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศ ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

#### ข้อ 4. การกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัทฯ ต้องจัดให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศแนวปฏิบัติ

ดังกล่าวให้ผู้เกี่ยวข้องรับทราบ โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องครอบคลุมการรักษาความมั่นคงปลอดภัย ด้านองค์กร ด้านบุคลากร ด้านกายภาพ และด้านเทคโนโลยี

ข้อ 5. การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ บริษัทฯ ต้องจัดให้มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง

ข้อ 6. การปฏิบัติตามระเบียบด้านความปลอดภัยสารสนเทศ บุคลากรทุกคนของบริษัทฯ ต้องปฏิบัติตามระเบียบด้านความปลอดภัยสารสนเทศอย่างเคร่งครัด ผู้ฝ่าฝืนจะมีความผิด และต้องได้รับการลงโทษทางวินัยตามแนวปฏิบัติการลงโทษของบริษัทฯ

ข้อ 7. การรายงานการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านสารสนเทศ ให้มีการรายงานการปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านสารสนเทศ รวมถึงระเบียบและข้อกำหนดใด ๆ ต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือรายงานโดยทันทีในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านสารสนเทศ

นโยบายฉบับนี้ให้ใช้บังคับกับบุคลากรทุกคนของบริษัทฯ และบุคคลอื่น ๆ ที่บริษัทฯ อนุมัติให้ใช้ระบบสารสนเทศของบริษัทฯ โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 16 เดือน สิงหาคม พ.ศ. 2566 เป็นต้นไป

- For www.rabbitholdings.co.th Only -