

ประกาศ
นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Policy Statement)

ตามที่ฝ่ายเทคโนโลยีสารสนเทศ ได้มีการจัดทำระบบการบริหารจัดการเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001 จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสื่อสารให้บุคลากรของฝ่ายเทคโนโลยีสารสนเทศ รวมถึงผู้ที่เกี่ยวข้องได้รับทราบนโยบาย และแนวทางปฏิบัติ เพื่อสร้างความตระหนัก และสามารถปฏิบัติงานได้อย่างสอดคล้อง โดยฝ่ายเทคโนโลยีสารสนเทศจะมีการทบทวนความเหมาะสมของนโยบายเป็นประจำทุกปี ซึ่งนโยบายจะกำหนดเป็นกรอบในการกำหนดวัตถุประสงค์เป้าหมายของแต่ละหน่วยงานในการให้บริการตามขอบข่ายการขอรับรองระบบ จึงมีการกำหนดนโยบายตามวิสัยทัศน์ ดังต่อไปนี้

“ฝ่ายเทคโนโลยีสารสนเทศเป็นองค์กรที่เป็นศูนย์กลางในการดำเนินการ และให้บริการด้านเทคโนโลยีดิจิทัล ที่มีความมั่นคงปลอดภัย และได้มาตรฐานสากล เพื่อสนับสนุนการดำเนินการตามพันธกิจของบริษัท แพลนเน็ต คอมมิวนิเคชั่น เอเชีย จำกัด (มหาชน)”

ฝ่ายเทคโนโลยีสารสนเทศ ขอประกาศแนวทางปฏิบัติเพื่อให้สอดคล้องตามนโยบาย ดังนี้

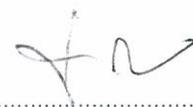
1. กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และให้การสนับสนุนในเรื่องงบประมาณ ทรัพยากร ความรู้ ความเข้าใจแก่บุคลากร
2. กำหนดแนวทางปฏิบัติที่เกี่ยวข้องในเรื่องของการรักษาความลับ (Confidentiality) โดยการทำสัญญาการรักษาความลับ, การรักษาความถูกต้อง ความสมบูรณ์ (Integrity) กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่ที่เกี่ยวข้อง, ความพร้อมใช้งาน (Availability) มีระบบอุปกรณ์สำรอง, การกำหนดสิทธิการเข้าออกพื้นที่เพื่อป้องกันการโจรกรรมข้อมูล กำหนดรหัสการเข้าใช้งาน และปรับปรุงตามนโยบายองค์กร
3. สื่อสาร ให้ความรู้ความเข้าใจด้านกฎหมาย ข้อบังคับ ข้อตกลงที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ ความต่อเนื่อง ข้อมูลความปลอดภัย
4. แต่งตั้งคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีการขับเคลื่อนนโยบาย และรักษาระบบการบริหารงานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง
5. กำหนดเป็นหัวข้อการอบรมปฐมนิเทศบุคลากรใหม่ และทบทวนในที่ประชุมฝ่ายเทคโนโลยีสารสนเทศประจำปี
6. ดำเนินการซักซ้อมแผนความต่อเนื่อง พัฒนา ปรับปรุง ทดสอบให้เหมาะสมและมั่นใจว่าพร้อมรับในทุกสถานการณ์



7. มีการทำข้อตกลงกับผู้ให้บริการภายนอก ผู้ขายอุปกรณ์ ในการให้ความร่วมมือเมื่อเกิดอุบัติเหตุการณีส่งผลกระทบต่อความปลอดภัยด้านข้อมูลสารสนเทศในการให้บริการ และทบทวนข้อตกลงปีละ 1 ครั้ง
 8. ผู้ที่เกี่ยวข้องทำการวางแผน และจัดการเรื่องความปลอดภัยของข้อมูล ระบบโครงข่าย เครื่องมือ และอุปกรณ์ให้อยู่ในระบบมาตรฐาน ซึ่งเป็นที่ยอมรับและเชื่อถือได้ รวมทั้งให้การดูแลเป็นพิเศษ
 9. การเก็บรักษาความปลอดภัยของข้อมูล จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่ฝ่ายเทคโนโลยีสารสนเทศทำกับผู้ให้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งจะต้องถือปฏิบัติโดยเคร่งครัด
 10. มาตรการเกี่ยวกับความปลอดภัยของข้อมูล ถือเป็นหน้าที่ของบุคลากรของฝ่ายเทคโนโลยีสารสนเทศทุกคน จะต้องปฏิบัติตาม และหากมีการฝ่าฝืน ให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง โดยฝ่ายเทคโนโลยีสารสนเทศถือเป็นหน้าที่ที่ต้องแจ้งให้บุคลากรทุกคนทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล
 11. ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ในการจัดเก็บ และเก็บรักษาข้อมูลของผู้ใช้บริการตามแบบ และวิธีการที่ได้ทำความตกลงร่วมกันไว้ระหว่างฝ่ายเทคโนโลยีสารสนเทศกับผู้ให้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใดๆ ที่มีได้รับความยินยอมจากผู้ใช้บริการสู่สาธารณชน หรือบุคคลภายนอก เพื่อไม่มีการรั่วไหล หรือการสูญหายของข้อมูลของผู้ใช้บริการ ไม่ว่าในกรณีใดๆ
 12. ฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่าบุคลากรจะไม่นำข้อมูลของฝ่ายเทคโนโลยีสารสนเทศหรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอก หรือที่ใดๆ หากมิได้รับความยินยอมจากฝ่ายเทคโนโลยีสารสนเทศหรือจากผู้ให้บริการ
- นโยบายและแนวปฏิบัตินี้ บุคลากรของฝ่ายเทคโนโลยีสารสนเทศจะต้องให้ความร่วมมือ และถือปฏิบัติร่วมกัน เพื่อให้มั่นใจว่าฝ่ายเทคโนโลยีสารสนเทศจะรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และมีการปรับปรุงประสิทธิภาพอย่างต่อเนื่อง

จึงประกาศมาเพื่อทราบ และยึดถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 1 กุมภาพันธ์ 2566



(นาย ประพัฒน์ รัฐเลิศกานต์)

กรรมการผู้อำนวยการและประธานเจ้าหน้าที่บริหาร

