ความมั่นคงปลอดภัยทางไซด์เบอร์ และกฎหมายที่เกี่ยวข้อง

นายอรรถกร วงค์อนันต์
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

หัวข้อที่นำเสนอ

- ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รพ.พระศรีฯ
- แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ
- พระราชบัญญัติคอมพิวเตอร์ 2560
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รพ.พระศรีฯ

ประกาศโรงพยาบาลพระศรีมหาโพธิ์
เรื่อง นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Policy Statement)

ด้วยโรงพยาบาลพระศรีมหาโพธิ์มีนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยมีเป้าหมายเพื่อป้องกันสินทรัพย์สารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้น ทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม

ดังนั้น เพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของโรงพยาบาลพระศรีมหาโพธิ์ ในการบริหารความมั่นคงปลอดภัยสารสนเทศ จึงประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ดังนี้

"สารสนเทศพระศรีมหาโพธิ์ พร้อมใช้ ปลอดภัย มั่นคง ก้าวไกล ได้มาตรฐานสากล"
(Prasri. Information Secure Safety Ready Advance International Standard)

ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รพ.พระศรีฯ

แนวทางปฏิบัติเพื่อให้สอดคล้องตามนโยบายมีดังนี้

๑. กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และให้การสนับสนุนในเรื่องงบประมาณ ทรัพยากร ความรู้ความเข้าใจแก่บุคลากร

๒. กำหนดแนวทางปฏิบัติที่เกี่ยวข้องในเรื่องของการรักษาความลับ (Confidentiality) โดยการทำสัญญารักษาความลับ, การรักษาความถูกต้อง ความสมบรูณ์ (Integrity) กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่ที่เกี่ยวข้อง, ความพร้อมใช้งาน (Availability) มีระบบอุปกรณ์สำรอง, การกำหนดสิทธิการเข้าออกพื้นที่เพื่อป้องกันการโจรกรรมข้อมูล กำหนดรหัสการเข้าใช้งาน และปรับปรุงตามนโยบายองค์กร

๓. สื่อสาร ให้ความรู้ความเข้าใจด้านกฎหมาย ข้อบังคับ ข้อตกลงที่เกี่ยวข้องกับการให้บริการด้านเทคโนโลยีสารสนเทศ ความต่อเนื่อง ข้อมูลความปลอดภัย

๔. แต่งตั้งคณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีการขับเคลื่อนนโยบาย และรักษาระบบการบริหารงานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง

๕. กำหนดเป็นหัวข้อการอบรมปฐมนิเทศบุคลากรใหม่ และทบทวนในที่ประชุมฝ่ายเทคโนโลยีและสารสนเทศประจำปี

๖. ดำเนินการซักซ้อมแผนความต่อเนื่อง พัฒนา ปรับปรุง ทดสอบให้เหมาะสมและมั่นใจว่าพร้อมรับในทุกสถานการณ์

๗. มีการทำข้อตกลงกับผู้ให้บริการภายนอก ผู้ขายอุปกรณ์ ในการให้ความร่วมมือเมื่อเกิดอุบัติการณ์ที่ส่งผลต่อความปลอดภัยด้านข้อมูลสารสนเทศในการให้บริการ และทบทวนข้อตกลงปีละ ๑ ครั้ง

ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ รพ.พระศรีฯ

๘. ผู้ที่เกี่ยวข้องทำการวางแผน และจัดการเรื่องความปลอดภัยของข้อมูล ระบบโครงข่าย เครื่องมือ และอุปกรณ์ ให้อยู่ในระบบมาตรฐานซึ่งเป็นที่ยอมรับและเชื่อถือได้ รวมทั้งให้การดูแลเป็นพิเศษ

๙. การเก็บรักษาความปลอดภัยของข้อมูล จะต้องระบุไว้เป็นส่วนหนึ่งในสัญญาบริการที่ฝ่ายเทคโนโลยีและสารสนเทศ ทำกับผู้ใช้บริการ ไม่ว่าจะเป็นการบริการประเภทใด ซึ่งจะต้องถือปฏิบัติโดยเคร่งครัด

๑๐. มาตรการเกี่ยวกับความปลอดภัยของข้อมูล ถือเป็นหน้าที่ของบุคลากรของฝ่ายเทคโนโลยีและสารสนเทศทุกคนจะต้องปฏิบัติตาม หากมีการฝ่าฝืนให้ถือว่าเป็นการกระทำผิดวินัยอย่างร้ายแรง โดยฝ่ายเทคโนโลยีและสารสนเทศถือเป็นหน้าที่ที่จะต้องแจ้งให้บุคลากรทุกคนทราบถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล

๑๑. ฝ่ายเทคโนโลยีและสารสนเทศ มีหน้าที่ในการจัดเก็บและเก็บรักษาข้อมูลของผู้ใช้บริการตามแบบ และวิธีการที่ได้ทำความตกลงร่วมกันไว้ระหว่างฝ่ายเทคโนโลยีและสารสนเทศกับผู้ใช้บริการ รวมทั้งการไม่เปิดเผยข้อมูลใดๆ ที่มิได้รับความยินยอมจากผู้ใช้บริการสู่สาธารณชน หรือบุคคลภายนอก เพื่อไม่มีการรั่วไหล หรือการสูญหายของข้อมูลของผู้ใช้บริการ ไม่ว่าในกรณีใดๆ

๑๒. ฝ่ายเทคโนโลยีและสารสนเทศ จะต้องจัดทำเอกสารที่ระบุไว้อย่างชัดเจนว่าบุคลากรจะไม่นำข้อมูลของฝ่ายเทคโนโลยีและสารสนเทศหรือข้อมูลของผู้ใช้บริการไปเปิดเผยแก่บุคคลภายนอก หรือที่ใดๆ หากมิได้รับความยินยอมจากฝ่ายเทคโนโลยีและสารสนเทศหรือจากผู้ใช้บริการ

๑๓. ฝ่ายเทคโนโลยีและสารสนเทศ จะมีการทบทวนนโยบายอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่านโยบายยังมีความเหมาะสมอยู่เสมอ

นโยบายและแนวปฏิบัตินี้ บุคลากรของฝ่ายเทคโนโลยีและสารสนเทศจะต้องให้ความร่วมมือและถือปฏิบัติร่วมกัน เพื่อให้มั่นใจว่าฝ่ายเทคโนโลยีและสารสนเทศจะรักษาความมั่นคงปลอดภัยด้านสารสนเทศและมีการปรับปรุงประสิทธิภาพอย่างต่อเนื่อง

ประกาศ ณ วันที่ ๒๑ มีนาคม พ.ศ. ๒๕๖๕

(นายประภาส อุครานันท์)
ผู้อำนวยการโรงพยาบาลพระศรีมหาโพธิ์

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

โรงพยาบาลพระศรีมหาโพธิ์

คู่มือปฏิบัติงาน

เรื่อง แนวทางปฏิบัติการรักษาความมั่นคง
ปลอดภัยสารสนเทศ

HB – ISMS - 01

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

	คู่มือปฏิบัติงานโรงพยาบาลพระศรีมหาโพธิ์ เรื่อง แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัย สารสนเทศ	เอกสารเลขที่ HB - ISMS - 01 ฉบับ A แก้ไขครั้งที่ 00 วันที่ 21 มีนาคม 2565 หน้าที่ 1 ของ 32 หน้า

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวดที่ 1

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

วัตถุประสงค์

1. เพื่อกำหนดการเข้าถึงข้อมูลสารสนเทศโดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัยด้านสารสนเทศ
2. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิและการมอบอำนาจของหน่วยงานของรัฐ

นโยบาย

บุคลากรโรงพยาบาลพระศรีมหาโพธิ์และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวดที่ 2
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน(User)ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย
2. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานแล้ว

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

3. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

4. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุมโดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยนรหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน

5. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยทุก 6 เดือน หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

6. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

7. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 3
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

1. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)
2. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์ และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

3. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

4. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. 2544

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 4
การควบคุมการเข้าถึงเครือข่าย
(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2. กำหนดแนวปฏิบัติการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายระบบคอมพิวเตอร์และระบบสารสนเทศของโรงพยาบาลพระศรีมหาโพธิ์ได้

3. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

4. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

5. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in Networks) โดยต้องแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภทของเครือข่าย

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

6. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ และการส่งข้อมูลสารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

7. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 5
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย
2. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน (User) ได้ และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งาน (User) ที่ได้รับอนุญาต
3. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน (Password Management System) โดยต้องจัดทำระบบบริหารจัดการรหัสผ่าน (Password) ที่สามารถทำงานเชิงโต้ตอบ (Interactive)หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่าน (Password) ที่มีคุณภาพ
4. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้
5. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)
6. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 6
การการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

1. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application and Information Access Control) ตามสิทธิ์ที่กำหนดไว้
2. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนมีผลกระทบ และมีความสำคัญสูงต่อโรงพยาบาลพระศรีมหาโพธิ์ โดยต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking)

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

3. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้อง ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
4. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 7
การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลพระศรีมหาโพธิ์ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินและการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง แม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

นโยบาย

1. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน
2. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลพระศรีมหาโพธิ์ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
3. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่องของโรงพยาบาลพระศรีมหาโพธิ์ด้านสารสนเทศ
4. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผน
5. บริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของโรงพยาบาลพระศรีมหาโพธิ์อย่างน้อยปีละ 1 ครั้ง
6. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 8
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนด มีความมั่นคงปลอดภัย และหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

1. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information SecurityAudit and Assessment) อย่างน้อยปีละ 1 ครั้ง
2. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายใน(Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 9
การบริหารจัดการและรักษาความลับข้อมูลสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการจัดการบริหารจัดการและการรักษาความลับข้อมูลสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนด สามารถแบ่งประเภทของข้อมูลสารสนเทศที่เป็นข้อมูลทั่วไป ข้อมูลความลับ และข้อมูลสำคัญ ให้มีการบริหารจัดการที่ดี สามารถส่งต่อข้อมูล และเปิดเผยข้อมูลให้เฉพาะผู้ที่มีสิทธิ์ในการเข้าถึงได้อย่างปลอดภัย สามารถนำข้อมูลไปใช้ให้เกิดประโยชน์สูงสุด

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

นโยบาย

1. กำหนดให้มีคณะกรรมการธรรมภิบาลข้อมูลโรงพยาบาลพระศรีมหาโพธิ์ เพื่อบริหารจัดการควบคุมตรวจสอบการใช้ข้อมูลสารสนเทศของโรงพยาบาล

2. กำหนดสิทธิ์การเข้าถึงข้อมูล และกำหนดลำดับชั้นข้อมูลที่ผู้ใช้สามารถเข้าถึงได้ การจัดเก็บข้อมูล การคัดลอกข้อมูล การโอนถ่ายข้อมูล การส่งต่อข้อมูล ช่องทางวิธีการในการรับส่งข้อมูล เพื่อป้องกันให้มีความปลอดภัยสารสนเทศในการใช้ข้อมูล ได้อย่างถูกต้อง เหมาะสม

3. ทบทวนกำกับติดตามข้อกำหนดในการเข้าถึงข้อมูลสารสนเทศ สิทธิ์การเข้าถึง ประเภทข้อมูล ระดับความลับข้อมูล วิธีการจัดเก็บ การโอนถ่าย การส่งต่อ รูปแบบช่องทางที่ใช้ส่งต่อข้อมูลสารสนเทศ

แนวปฏิบัติในการรักษาความมั่นคงปลอดสารสนเทศ

หมวด 10
การจัดการสื่อที่ใช้บันทึกข้อมูลสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการจัดการบริหารจัดการสื่อที่ใช้บันทึกข้อมูลสารสนเทศให้สามารถได้อย่างถูกต้อง เหมาะสม ปลอดภัย มีความพร้อมใช้งาน ป้องกันความเสี่ยงในการใช้งานผิดประเภท ป้องกันการใช้บันทึกสื่อที่มีความเสียงต่อความปลอดภัยสารสนเทศ ป้องการความเสี่ยหายที่อาจจะเกิดกับสื่อบันทึกข้อมูลสารสนเทศ

นโยบาย

1. กำหนดแนวทางในการบริหารจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้เกิดความปลอดภัยด้านสารสนเทศ
2. กำหนดแนวทางการตรวจสอบการใช้งานสื่อบันทึกข้อมูล ให้มีความปลอดภัยด้านสารสนเทศ

พระราชบัญญัติคอมพิวเตอร์ 2560

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

พระราชบัญญัติคอมพิวเตอร์ 2560

พ.ร.บ.คอมพิวเตอร์ หรือ พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับล่าสุดได้มีการประกาศใช้เมื่อเดือนพฤษภาคม พ.ศ.2560 ซึ่งเป็น พ.ร.บ. คอมพิวเตอร์ ฉบับที่ 2

สำหรับคนที่ต้องใช้งานคอมพิวเตอร์เป็นประจำ หรือทำงานเกี่ยวกับโลกออกไลน์ต้องพึงรู้ไว้เลยค่ะ เพราะหากใช้ไม่ระวัง เราอาจจะเผลอทำผิดกฎหมายได้

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

พ.ร.บ.คอมพิวเตอร์ คืออะไร

พ.ร.บ.คอมพิวเตอร์ คือพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งคอมพิวเตอร์ที่ว่านี้ก็เป็นได้ทั้งคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์โน้ตบุ๊ค สมาร์ตโฟน รวมถึงระบบต่างๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ด้วย ซึ่งเป็นพ.ร.บ.ที่ตั้งขึ้นมาเพื่อป้องกันควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ หากใครกระทำความผิดตามพ.ร.บ.คอมพิวเตอร์นี้ ก็จะต้องได้รับการลงโทษตามที่พ.ร.บ.กำหนดไว้

ประเทศไทย มี พ.ร.บ. คอมพิวเตอร์ มาแล้ว 2 ฉบับ คือ ฉบับแรก ปี 2550 และ ฉบับสอง ปี 2560 โดยฉบับที่ใช้งานปัจจุบัน คือ ฉบับปี 2560

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

พ.ร.บ.คอมพิวเตอร์ 2560 มีอยู่ 2 หมวด โดยหมวดที่เกี่ยวข้องกับประชาชน คือ หมวด 1 “ความผิดเกี่ยวกับคอมพิวเตอร์” เพราะเป็นหมวดที่บอกว่า พฤติกรรมใดที่มีความผิด พ.ร.บ.คอมพิวเตอร์ และมีบทลงโทษอะไรอย่างไร

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 5	ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
มาตรา 6	ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 7	ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 8	ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 9	ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือ บางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 10	ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 11	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ บุคคลอื่นโดยปกติสุข	-	ไม่เกิน 100,000 บาท
	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย	-	ไม่เกิน 200,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 12	ถ้าการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ	ตั้งแต่ 1 ปี- 7 ปี	20,000 บาท-140,000 บาท
	ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว	ตั้งแต่ 1 ปี- 10 ปี	20,000 บาท-200,000 บาท
	ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง	ตั้งแต่ 3 ปี- 15 ปี	60,000 บาท-300,000 บาท
	ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่าแต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย	ตั้งแต่ 5 ปี- 20 ปี	100,000 บาท-400,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 12/1	ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น	ไม่เกิน 10 ปี	ไม่เกิน 200,000 บาท
	ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 โดยมิได้มีเจตนาฆ่าแต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย	ตั้งแต่ 5 ปี- 20 ปี	100,000 บาท-400,000 บาท
มาตรา 13	ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือ มาตรา 11	ไม่เกิน 5 ปี	20,000 บาท
	ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 12 วรรคหนึ่งหรือวรรคสาม	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 14 (1)	นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 14 (2)	นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 14 (3)	นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 14 (4)	นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 14 (5)	ผู้ใดเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตาม (1) (2) (3) หรือ (4)	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

โดยหมวด 1 มีมาตราที่ควรสนใจทั้งหมด 11 มาตราดังนี้

มาตรา	ความผิด พ.ร.บ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
มาตรา 15	ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด ตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 16	ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	ไม่เกิน 3 ปี	ไม่เกิน 200,000 บาท
	ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย	ไม่เกิน 3 ปี	ไม่เกิน 200,000 บาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 5

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 9

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 11

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 12

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 13

พ.ร.บ.คอมพิวเตอร์ มาตราที่ 14

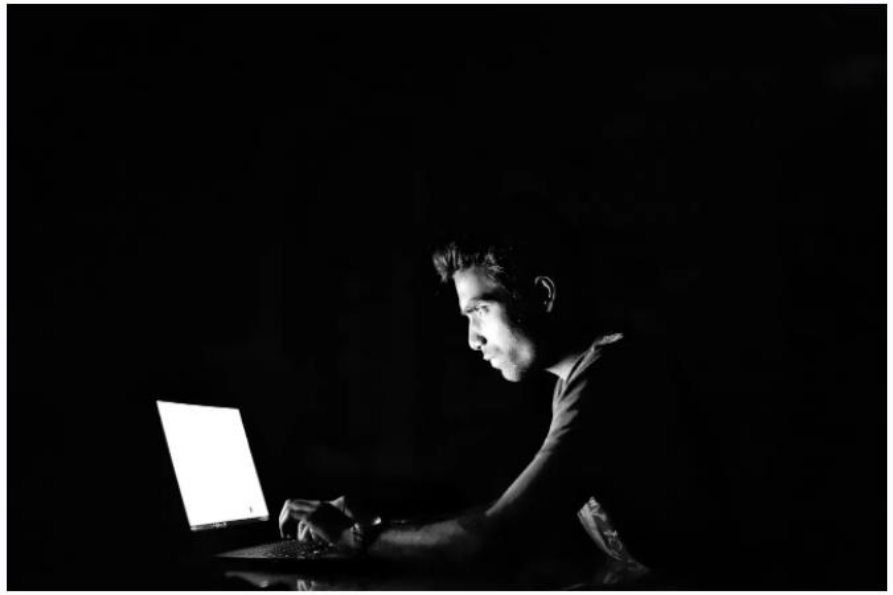
พ.ร.บ.คอมพิวเตอร์ มาตราที่ 16

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 5 | ตัวอย่างการกระทำผิด



การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตัวอย่างเช่น

- การแฮคเกอร์ เข้าไปดูข้อมูลคอมพิวเตอร์คนอื่น โดยไม่ได้รับอนุญาต
- การใช้ username / password ของผู้อื่น Login เข้าสู่ระบบ โดยไม่ได้รับการอนุญาต

บทลงโทษ

ต้องระวางโทษ จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 9 | ตัวอย่างการกระทำผิด

ทำลาย แก้ไข ดัดแปลง นำไฟล์อันตรายเข้าสู่คอม จนทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย ตัวอย่างเช่น

- การนำไฟล์อันตราย เช่น ไวรัส มัลแวร์ มาสู่คอมพิวเตอร์ของเพื่อน หรือ คนรู้จัก จนระบบคอมพิวเตอร์เสียหาย
- การแฮคเกอร์ เข้าไปดูข้อมูลคอมพิวเตอร์คนอื่น โดยไม่ได้รับอนุญาต
- การใช้ username / password ของผู้อื่น Login เข้าสู่ระบบ โดยไม่ได้รับการอนุญาต

บทลงโทษ

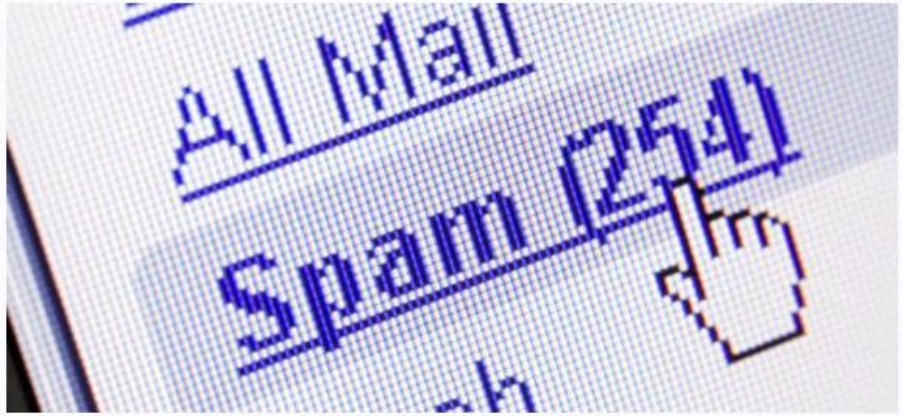
ต้องระวางโทษ จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 11 | ตัวอย่างการกระทำผิด



มาตรานี้เกี่ยวข้องโดยตรงกับพ่อค้าแม่ค้าออนไลน์ค่ะ เพราะเกี่ยวข้องกับการโปรโมทสินค้าบนอินเตอร์เน็ต โดยการกระทำที่อาจผิด พ.ร.บ. คอมพิวเตอร์ 2560 มีดังนี้

- **การส่งข้อมูลหรืออีเมล์ก่อกวนผู้อื่น (สแปม)** เพื่อขายสินค้าหรือบริการ จนผู้รับเกิดความเดือดร้อนรำคาญ โดยไม่มีปุ่มให้กดเลิกการรับอีเมล์
- การฝากร้านใน FB หรือ IG แบบรัวๆ ซ้ำไปซ้ำมา โดยเจ้าของเพจไม่ได้อนุญาต จนเกิดความเดือดร้อนรำคาญแก่เจ้าของเพจหรือผู้พบเห็น

บทลงโทษ

ต้องระวางโทษ ปรับไม่เกิน 2 แสนบาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 12 | ตัวอย่างการกระทำผิด

กระทำการทำลาย แก้ไข หรือ รบกวนข้อมูลหรือระบบคอมพิวเตอร์ ของระบบสาธารณะ หรือ ความมั่นคง เช่น

- เจาะเข้าระบบคอมพิวเตอร์ซึ่งความคุมไฟฟ้าในนครหลวง และสั่งดับไฟฟ้าทั่วเมือง อันก่อให้เกิดความวุ่นวายและมีผลกระทบเป็นวงกว้าง

บทลงโทษ

ต้องระวางโทษ ปรับไม่เกิน 2 แสนบาท

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 13 | ตัวอย่างการกระทำผิด

จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด ตัวอย่างเช่น

- เป็นผู้จำหน่ายชุดคำสั่งที่ใช้ในการเจาะระบบ หรือ รบกวนข้อมูลคอมพิวเตอร์ เช่น โปรแกรมทำ BOTNET หรือ DOS (Denial of Service)

บทลงโทษ

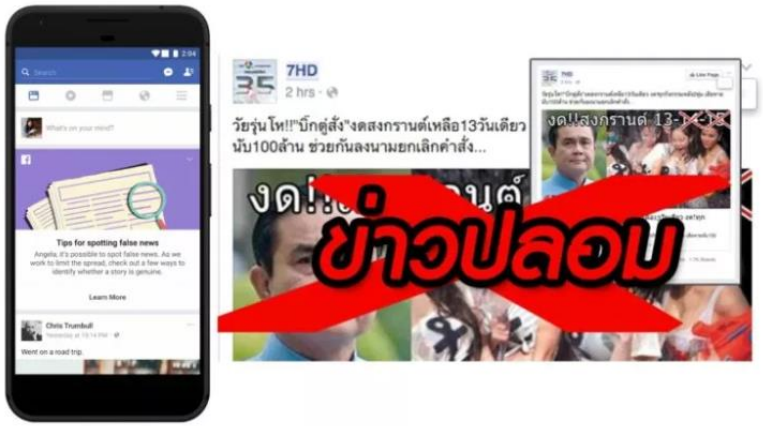
ต้องระวางโทษ จำคุกไม่เกิน 5 ปี เดือน ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ

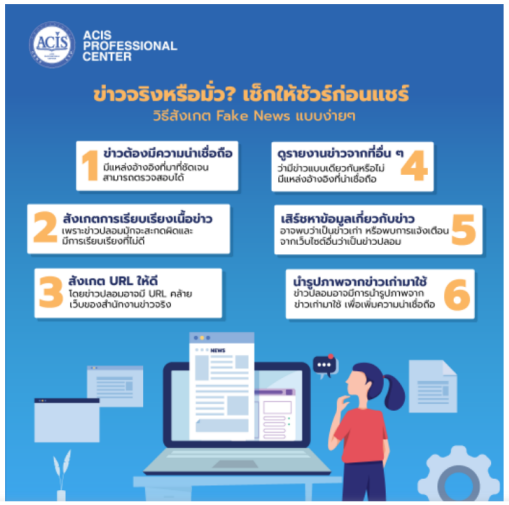
ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 14 | ตัวอย่างการกระทำผิด





พ.ร.บ. คอมพิวเตอร์ มาตรา 14 คือหนึ่งในมาตราที่ประชาชนควรให้สนใจเป็นพิเศษ เพราะเป็นหนึ่งในฐานความผิดที่มีคดีฟ้องร้องมากที่สุด โดยตัวอย่างการกระทำผิด มาตราดังกล่าว มีดังนี้

- โพสต์หรือแชร์ ข้อมูลปลอม ไม่เป็นความจริง หลอกลวง (อย่างเช่น **แม่ค้าออนไลน์โพสต์หลอกลวงเพื่อเก็บเงินลูกค้า** แต่ไม่มีการส่งมอบสินค้าจริง โฆษณาธุรกิจลูกโซ่ที่หลอกลวงเอาเงินลูกค้า โพสข่าวปลอม เป็นต้น)
- การกด like & Share ข่าวหรือข้อมูลปลอม อันเป็นการให้เพื่อนใน social network ได้เห็นข้อมูลดังกล่าวด้วย ก็ถือเป็นความผิดตาม พรบ คอมพิวเตอร์ มาตรา 14 เช่นกัน
- เป็นแอดมินเพจที่ปล่อยให้มีข่าวหรือข้อมูลปลอมเผยแพร่ในเพจตัวเอง โดยมิได้ทำการลบทิ้ง
- โพสหรือเผยแพร่ภาพเปลือย ภาพลามกอนาจารของคนรู้จัก หรือ คนรักเก่า อันเป็นเหตุให้ผู้อื่นได้รับความอับอายหรือเสียหาย

บทลงโทษ

หากเป็นการกระทำที่ส่งผลถึงประชาชน ต้องได้รับโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ และหากเป็นกรณีที่เป็นการกระทำที่ส่งผลต่อบุคลใดบุคคลหนึ่ง ต้องได้รับโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ (แต่ในกรณีอย่างหลังนี้สามารถยอมความกันได้)

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

ตัวอย่าง การกระทำความผิดเกี่ยวกับ พรบ คอมพิวเตอร์ พร้อมบทลงโทษ

พ.ร.บ. คอมพิวเตอร์ มาตรา 16 | ตัวอย่างการกระทำผิด

กระทำการเผยแพร่ภาพที่สร้างขึ้น หรือภาพตัดต่อ อันเป็นเหตุให้ผู้อื่นได้รับการดูหมิ่น อับอาย หรือ เสียชื่อเสียง ตัวอย่างเช่น

- เผยแพร่ข้อมูลเยาวชน โดยไม่มีการปกปิดตัวตนของเยาวชนท่านนั้น โดยตามกฎหมาย หากเปิดเผยตัวตนเยาวชนสู่สาธารณะ อาจทำให้ใช้ชีวิตในสังคมลำบาก อาจถูกดูหมิ่น เกลียดชัง
- เผยแพร่ภาพของผู้เสียชีวิต อันส่งผลให้พ่อแม่หรือคู่สมรสของผู้ตาย เกิดความอับอาย

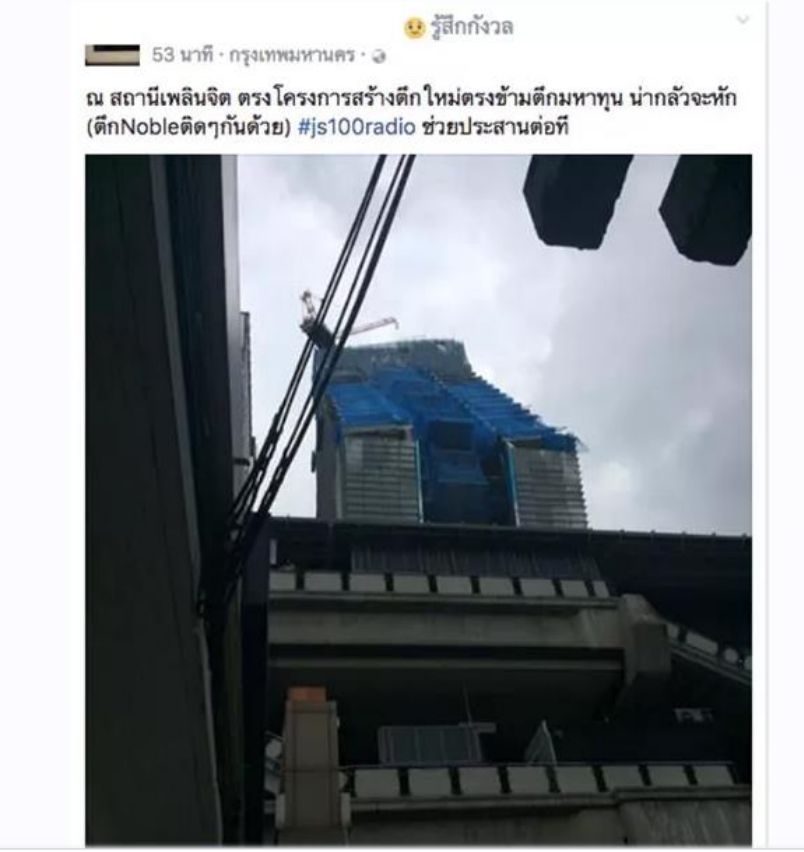
บทลงโทษ

ต้องระวางโทษ จำคุกไม่เกิน 3 ปี เดือน ปรับไม่เกิน 2 แสนบาท หรือทั้งจำทั้งปรับ

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

กรณีศึกษา: การทำผิดกฎหมายคอมพิวเตอร์ ตาม พ.ร.บ.คอมพิวเตอร์



เคสแรก เป็นเคสที่ออกข่าวอย่างโด่งดังเช่นกัน เป็นกรณีที่มีชายหนุ่มคนหนึ่งถ่ายรูปตึกที่มีลักษณะเอนๆ พร้อมโพสต์ข้อความประมาณว่า ตึกทรุดตัว ลงบน Facebook เลยทำให้เกิดเป็นประเด็นที่หลายเอาตกอกตกใจไปกันใหญ่ แต่ต่อมาก็มีการเปิดเผยว่า ตึกที่เห็นนั้นเป็นเพียงดีไซน์ของตึกที่ตั้งใจจะให้เอนแบบนั้นอยู่แล้ว เลยทำให้เจ้าของโพสต์ถูกตำรวจเรียกสอบสวน เพราะเข้าข่ายความผิด พ.ร.บ.คอมพิวเตอร์ ม.14 (2) นำข้อความเท็จเข้าระบบคอมพิวเตอร์ อันเป็นเท็จก่อให้เกิดความตื่นตระหนก

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคอมพิวเตอร์ 2560

พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2560 หรือฉบับที่ 2 ปัจจุบันมีผลบังคับใช้แล้ว ถ้าเราเป็นคนหนึ่งที่คลุกคลีกับการใช้งานคอมพิวเตอร์ หรืออินเตอร์เน็ต ก็ควรจะรู้เกี่ยวกับ พ.ร.บ. นี้ไว้ เพราะเราจะได้ไม่เผลอไปทำความผิด อย่างน้อยๆ ต้องระวัง 8 ประเด็น อีกทั้งการมี พ.ร.บ.คอมพิวเตอร์ ขึ้นมา ก็ถือว่าเป็นการควบคุมการใช้งานคอมพิวเตอร์ในระดับหนึ่ง และในทางหนึ่งก็ช่วยคุ้มครองสิทธิเสรีภาพของผู้ใช้งานด้วย

ที่มา:https://contentshifu.com/blog/computer-law

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

PDPA คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

PDPA ย่อมาจาก **Personal Data Protection Act B.E. 2562 (2019)** เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA Thailand (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อน **ให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565**

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๓๒ มาตรา ๓๓ และมาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒"

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่จะบังคับใช้ในประเทศไทยนี้ จะมีบทบาทในการคุ้มครองและให้สิทธิที่เราควรมีต่อข้อมูลส่วนบุคคลของเราเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บข้อมูลส่วนบุคคล, รวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งล้วนแล้วเกี่ยวข้องกับ พ.ร.บ. ฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษของ PDPA สำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ข้อมูลส่วนบุคคล คืออะไร?

ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว

ข้อมูลส่วนบุคคล (Personal Data) ได้แก่ ชื่อ-นามสกุล หรือชื่อเล่น / เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล) / ที่อยู่, อีเมล์, เลขโทรศัพท์ / ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID / ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม / ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน / ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ,สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน / ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ / ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง / ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file / ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

นอกจากนี้ยังมีข้อมูลส่วนบุคคลอีกประเภท ที่ พ.ร.บ. ฉบับนี้ให้ความสำคัญและมีบทลงโทษที่รุนแรงด้วยกรณีเกิดการรั่วไหลสู่สาธารณะ คือ **ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)** ได้แก่ ข้อมูล เชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ, ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

เหตุที่ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เป็นข้อมูลที่มีบทลงโทษที่รุนแรงกว่าข้อมูลส่วนบุคคลทั่วไป (Personal Data) เพราะหากข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนมีการรั่วไหลไปสู่สาธารณะแล้ว จะเกิดผลเสียที่ร้ายแรงกับผู้เป็นเจ้าของข้อมูลส่วนบุคคล(Data Subject)ได้มากกว่าข้อมูลส่วนบุคคลอื่นๆ มีผลต่อสิทธิเสรีภาพของบุคคล เช่น สิทธิเสรีภาพในความคิด ความเชื่อทางศาสนา การแสดงออก การชุมนุม สิทธิในชีวิตร่างกาย การอยู่อาศัย การไม่ถูกเลือกปฏิบัติ ซึ่งอาจจะก่อให้เกิดการแทรกแซงซึ่งสิทธิเสรีภาพและการเลือกปฏิบัติต่อการใช้สิทธิเสรีภาพของบุคคลได้มากกว่าข้อมูลส่วนบุคคลทั่วไป ยกตัวอย่างเช่น ข้อมูลพฤติกรรมทางเพศ เชื่อชาติ ศาสนา ประวัติอาชญากรรม ถ้ารั่วไหลไปแล้ว ข้อมูลเหล่านี้จะนำมาสู่ความเป็นอคติและจะมีผลกระทบต่อชีวิตส่วนบุคคลได้มากกว่าข้อมูลทั่วไปเป็นอย่างมาก

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ใครบ้างที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล?

เราสามารถแบ่งผู้ที่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล ในกฎหมาย PDPA ได้ 3 ประเภท ได้แก่

- **1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)** คือ บุคคลที่ข้อมูลสามารถระบุไปถึงได้
- **2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

แล้ว PDPA ให้เจ้าของข้อมูลส่วนบุคคล (Data Subject) ได้รับสิทธิอะไรบ้าง?

เพื่อให้ง่ายต่อความเข้าใจในสิทธิของเจ้าของข้อมูล(Data Subject) เรามาทำความรู้จักกับคำว่า **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** เพิ่มเติมอีกสักหน่อย

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คืออะไร ? ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึงบุคคลหรือนิติบุคคล ที่มีส่วนในการเก็บรวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคล และหากดูที่ความหมายอย่างละเอียดแล้ว นั่นหมายความว่าเพียงแค่เรามีการเก็บข้อมูลส่วนบุคคลของผู้อื่นไว้ ก็ถือว่าเราเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตามกฎหมาย PDPA ไปด้วยเหมือนกัน

ใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะให้ **สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)** สรุปได้ดังต่อไปนี้

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

สิทธิได้รับการแจ้งให้ทราบ

การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้ง ให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล (ยกเว้นเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว เช่น ไปธนาคารเพื่อจะไปเปิดบัญชี หรือว่าการสมัครใช้ผลิตภัณฑ์หรือบริการต่าง ๆ) โดยมีรายละเอียดการแจ้งให้ทราบ เช่น เก็บข้อมูลส่วนบุคคลอะไรบ้าง, วัตถุประสงค์การเก็บข้อมูล, การนำไปใช้หรือส่งต่อไปมีให้ใครบ้าง, วิธีเก็บข้อมูลอย่างไร, เก็บข้อมูลนานแค่ไหน, วิธีขอการเปลี่ยนแปลง แก้ไข เพิกถอนข้อมูลส่วนบุคคลที่ให้ไปสามารถทำได้อย่างไรบ้าง

สิทธิขอเข้าถึงข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิภายใน 30 วันนับจากวันที่ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ

สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ แต่ต้องไม่ขัดด้วยกฎหมายที่สำคัญยิ่งกว่า หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย หรือข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

สิทธิขอให้ลบหรือทำลาย

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเอง

สิทธิในการเพิกถอนความยินยอม

ถ้าเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไปแล้ว ต่อมาภายหลังต้องการยกเลิกความยินยอมนั้น ก็สามารถทำเมื่อใดก็ได้ และการยกเลิกความยินยอมนั้นจะต้องทำได้ง่ายเหมือนกับตอนแรกที่เจ้าของข้อมูลให้ความยินยอมด้วย โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้

สิทธิขอให้ระงับการใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล ไม่ว่าจะในกรณีที่เกิดการเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิ ก็สามารถทำได้

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย

สิทธิในการขอให้โอนข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกได้ทำจัดทำข้อมูลส่วนบุคคลของเราไปในอยู่ในรูปแบบต่างๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้ได้ หรือจะขอให้ส่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการและเทคนิค โดยการใช้สิทธินั้นต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ผู้ควบคุมข้อมูลส่วนบุคคล จะสามารถรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ก็ต่อเมื่อ?

บุคคลธรรมดา หรือนิติบุคคล (บริษัท ห้างร้าน มูลนิธิ สมาคม หน่วยงาน องค์กร ร้านค้า หรืออื่นใดก็ตาม) หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ หรือมีการนำข้อมูลส่วนบุคคลไปใช้ หรือนำไปเปิดเผยไม่ว่าจะวัตถุประสงค์ใดก็ตาม จำเป็นต้องได้รับ คำยินยอม (Consent) จากเจ้าของข้อมูลด้วย เว้นแต่จะเป็นไปตามข้อยกเว้นที่ พ.ร.บ.กำหนดไว้ โดยมีข้อยกเว้นดังต่อไปนี้

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ข้อยกเว้นที่ไม่ต้องมีคำยินยอมให้ข้อมูล ตาม พรบ กำหนดไว้

– จัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ที่เกี่ยวข้องกับ การศึกษาวิจัยหรือการจัดทำสถิติ

– เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

– จำเป็นเพื่อปฏิบัติตามสัญญากับเจ้าของข้อมูล เช่น การซื้อขายของออนไลน์ ต้องใช้ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล

– จำเป็นเพื่อประโยชน์สาธารณะ และการปฏิบัติหน้าที่ในการใช้อำนาจรัฐ

– จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลอื่น

– เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เช่น ส่งข้อมูลพนักงานให้กรมสรรพากรเรื่องภาษี เป็นต้น

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

ข้อยกเว้นที่ไม่ต้องมีคำยินยอมให้ข้อมูล ตาม พรบ กำหนดไว้

– เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

– การดำเนินกิจกรรมที่ชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของ มูลนิธิ สมาคม องค์กรไม่แสวงหากำไร เช่น เรื่องศาสนาหรือความคิดเห็นทางการเมือง ซึ่งจำเป็นต้องเปิดเผยให้ทราบก่อนเข้าองค์กรนั้น ๆ เป็นต้น

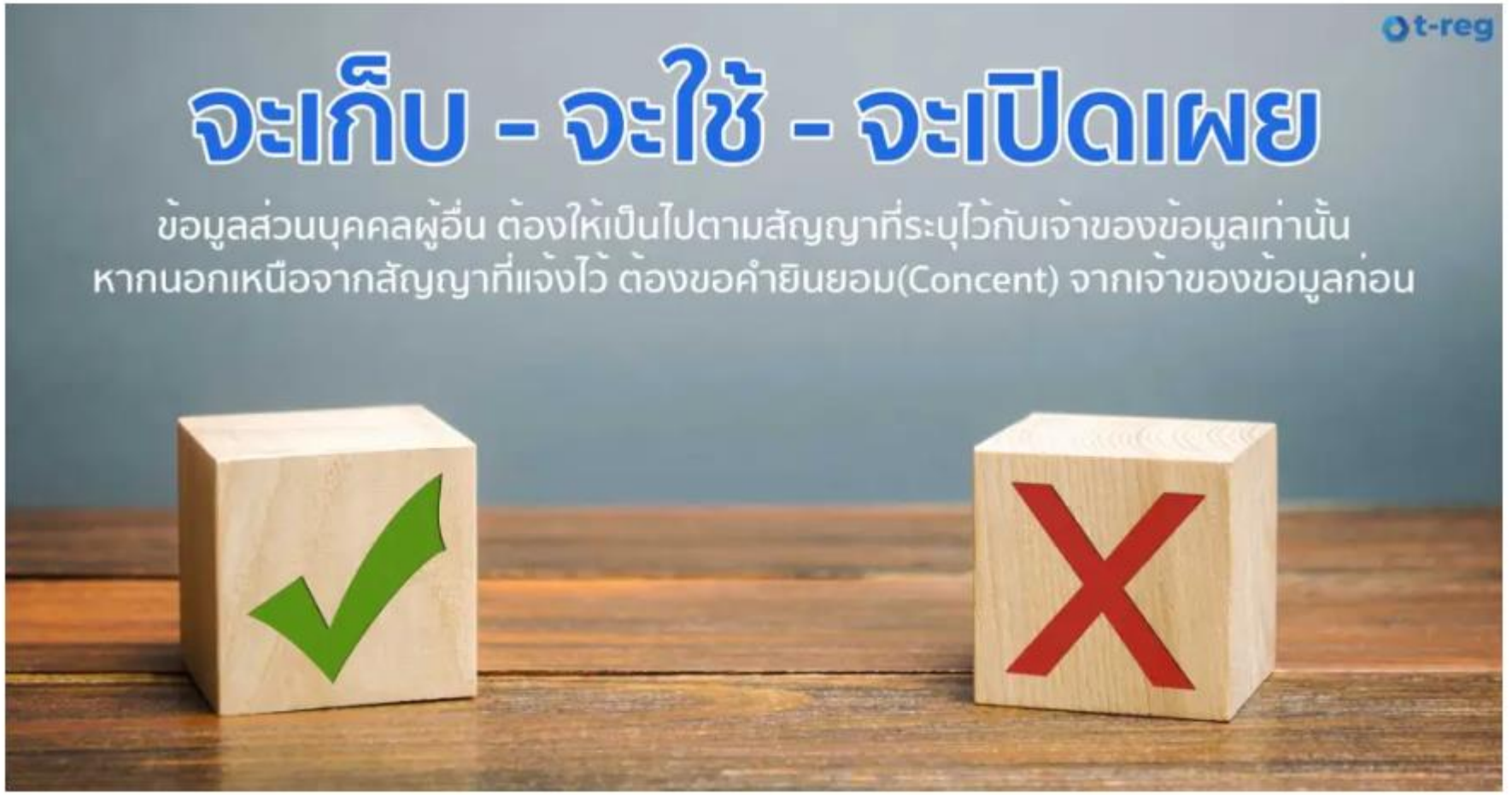
– เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล เช่น บุคคลสาธารณะที่มีข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วในความยินยอมของเจ้าของข้อมูล

– เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย เช่น เก็บลายนิ้วมือของผู้ที่บุกรุกเพื่อนำไปใช้ในชั้นศาล เป็นต้น

– เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ เกี่ยวกับ เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ เช่น การเก็บข้อมูลสุขภาพของพนักงานซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) องค์กรมักใช้ข้อนี้ในการอ้างสิทธิที่จำเป็นต้องเก็บข้อมูลนี้ไว้ เป็นต้น / ประโยชน์ด้านสาธารณะสุข, การคุ้มครองแรงงาน, การประกันสังคม, หลักประกันสุขภาพแห่งชาติ / การศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์, สถิติ, หรือประโยชน์สาธารณะอื่น / ประโยชน์สาธารณะที่สำคัญ

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)



ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

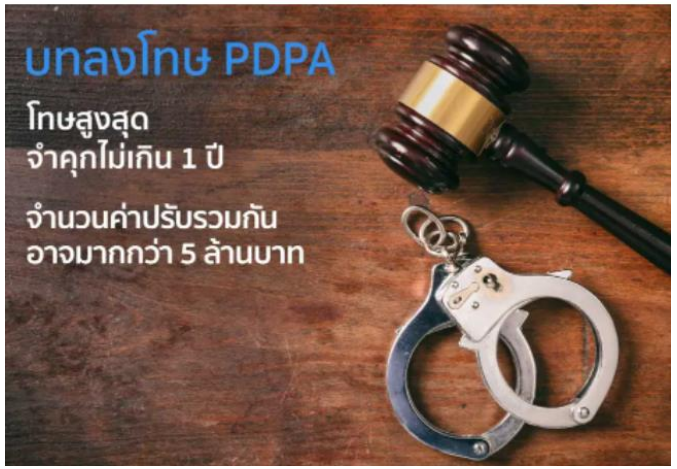
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

เมื่อ PDPA บังคับใช้แล้วแต่ไม่ได้ปฏิบัติตาม จะมีบทลงโทษอะไรบ้าง ?

ถ้าไม่ปฏิบัติตาม PDPA บทลงโทษของผู้ที่ไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) มีถึง 3 ประเภท ได้แก่

โทษทางแพ่ง

โทษทางแพ่งกำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง ตัวอย่าง หากศาลตัดสินว่าให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล เป็นจำนวน 1 แสนบาท ศาลอาจมีคำสั่งกำหนดค่าสินไหมเพื่อการลงโทษเพิ่มอีก 2 เท่าของค่าเสียหายจริง เท่ากับว่าจะต้องจ่ายเป็นค่าปรับทั้งหมด เป็นจำนวนเงิน 3 แสนบาท



โทษทางอาญา

โทษทางอาญาจะมีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ ประเภทข้อมูลที่มีความละเอียดอ่อน(Sensitive Personal Data) ส่วนกรณีหากผู้กระทำความผิด คือ บริษัท(นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ ผู้บริหาร, กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน

โทษทางปกครอง

โทษปรับ มี ตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อน(Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

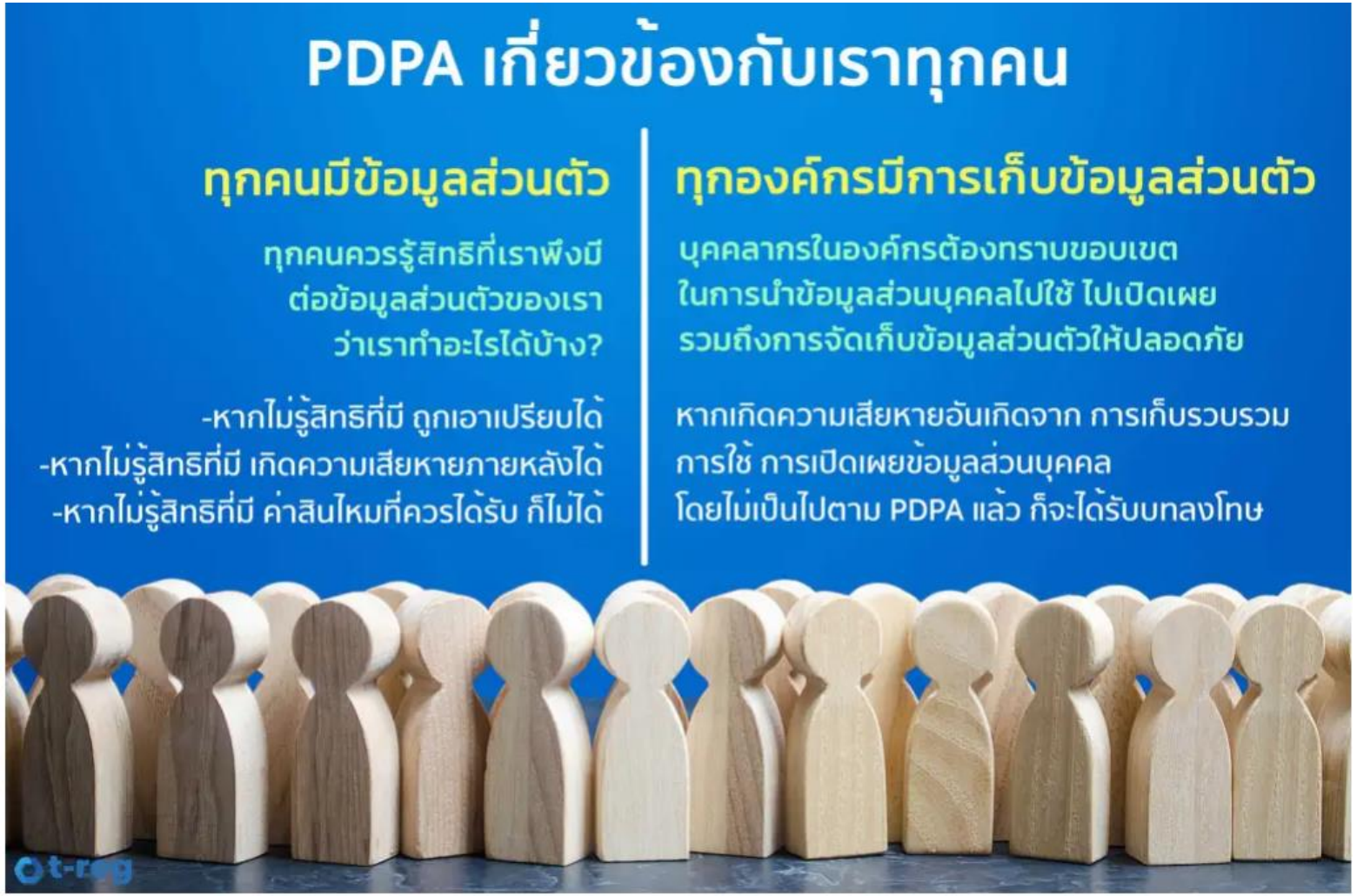
สรุปใจความสำคัญของ PDPA

จะเห็นได้ว่า PDPA หรือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีหัวใจสำคัญก็เพื่อต้องการรักษาสิทธิที่พึงมีแก่เจ้าของข้อมูล ว่าข้อมูล ส่วนตัวของเราจะปลอดภัย นำไปใช้อย่างถูกต้องเหมาะสมตามความต้องการและยินยอมของเจ้าของข้อมูลอย่างแท้จริง อย่างไรก็ตามผู้เป็นเจ้าของข้อมูลก็ควรพิจารณาอย่างรอบคอบเช่นกันว่าการให้ข้อมูลส่วนบุคคลในแต่ละครั้ง ***เป็นไปเพื่อวัตถุประสงค์อะไร? ข้อมูลที่ให้ไปมีเพียงพอกับวัตถุประสงค์นั้นแล้วหรือยัง?*** หากมองว่ามีการให้ข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องกับวัตถุประสงค์ของการขอข้อมูล เราก็สามารถปฏิเสธการให้ข้อมูลนั้นได้ เพื่อเป็นการป้องกันการนำข้อมูลไปใช้ในทางที่ผิดหรือหาผลประโยชน์จากข้อมูลส่วนบุคคลของเราก็เป็นได้

สำหรับในส่วนผู้เก็บข้อมูลนั้น นับว่าได้รับผลกระทบโดยตรงเป็นอย่างมากกับ PDPA ที่จะต้องปฏิบัติตาม ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคคลากรในองค์กร, รู้ขอบเขตการเก็บรวบรวม การใช้ การเผยแพร่ข้อมูลส่วนบุคคล, มีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย, มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคล, มีการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล สิ่งเหล่านี้ล้วนจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตามเพื่อให้สอดคล้องกับ PDPA ต่อไป มาถึงตรงนี้ผู้อ่านก็พอจะทราบแล้วว่า PDPA คืออะไรและเกี่ยวข้องกับเราอย่างไร

ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)



ที่มาhttps://t-reg.co/blog/t-reg-knowledge/what-is-pdpa/


THANK
YOU