**บทที่ 3 ทรัพย์สินทางปัญญา**

**ทรัพย์สินทางปัญญา คือ** ทรัพย์สินที่เกิดจากความคิดสร้างสรรค์และปัญญาของมนุษย์ ซึ่งสามารถนำมาใช้ประโยชน์ทางเศรษฐกิจได้ ได้แก่ ผลงานวรรณกรรม, การประดิษฐ์คิดค้น, การออกแบบ, เครื่องหมายการค้า, ตวามลับทางการค้า เป็นต้น

การคุ้มครองทรัพย์สินทางปัญญาเป็นการให้สิทธิพิเศษแก่เจ้าของทรัพย์สินในการใช้ประโยชน์จากผลงานหรือทรัพย์สินที่ตนสร้างขึ้น โดยป้องกันไม่ให้ผู้อื่นนำไปใช้โดยไม่ได้รับอนุญาต

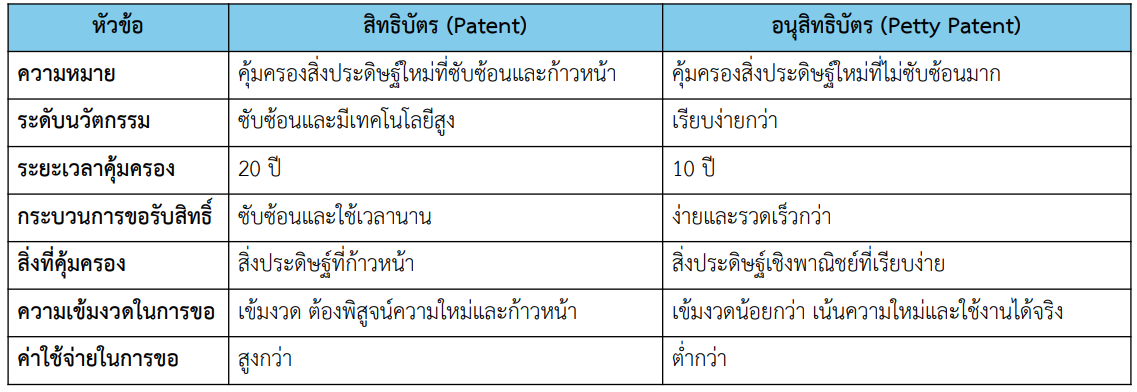
**ประเภทของทรัพย์สินทางปัญญา**

1. **สิทธิบัตรและอนุสิทธิบัตร**

สิทธิบัตรการประดิษฐ์(ใหม่ที่มีความคิดสร้างสรรค์)

สิทธิบัตรการออกแบบผลิตภัณฑ์(มีลักษณะเฉพาะ)

อนุสิทธิบัตร มีขั้นตอนการประดิษฐ์ที่ซับซ้อนน้อยกว่าสิทธิบัตร

****

1. **เครื่องหมายการค้า**

เป็นเครื่องหมายหรือสัญลักษณ์ที่ใช้ในการค้าเพื่อแยกแยะสินค้าหรือบริการของแต่ละองค์กร มีลักษณะเป็นโลโก้ ชื่อ สัญลักษณ์ หรือการออกแบบที่เป็นเอกลักษณ์

การจดทะเบียนเครื่องหมายการค้าเป็นการสื่อให้สิทธิ์ทางกฎหมายในการปกป้องเครื่องหมายการค้าจากการละเมิดสิทธิ์โดยผู้อื่น ทำให้สามารถใช้เครื่องหมายได้เพียงผู้เดียวและสามารถดำเนินการทางกฎหมายกับผู้ที่ละเมิดได้

* สิทธิและหน้าที่ของเจ้าของเครื่องหมายการค้า
* สิทธิในการใช้: เจ้าของเครื่องหมายการค้ามีสิทธิ์ในการใช้เครื่องหมายในการค้าแต่เพียงผู้เดียว
* สิทธิในการฟ้องร้อง: เจ้าของสามารถฟ้องร้องเรียกค่าเสียหายจากผู้ที่ละเมิดเครื่องหมายการค้าได้
* การรักษาสิทธิ์: เจ้าของต้องชำระค่าธรรมเนียมรายปีและใช้เครื่องหมายการค้าอย่างต่อเนื่องเพื่อรักษาสิทธิ์
* ประโยชน์ของการจดทะเบียนเครื่องหมายการค้า
* ป้องกันการละเมิด: ช่วยปกป้องเครื่องหมายการค้าจากการถูกละเมิดหรือเลียนแบบ
* สร้างความน่าเชื่อถือ: ส่งเสริมความน่าเชื่อถือและภาพลักษณ์ที่ดีของแบรนด์
* เพิ่มมูลค่า: เครื่องหมายการค้าที่แข็งแกร่งสามารถเพิ่มมูลค่าให้กับธุรกิจและสามารถนำไปใช้ในการขยายตลาดได้

**ประเภท**

* + เครื่องหมายการค้า เช่น samsung
  + เครื่องหมายบริการ เช่น facebook
  + เครื่องหมายรับรอง เช่น อย.
  + เครื่องหมายร่วม เช่น ptt, scg

1. **ความลับการค้า**

ข้อมูลที่มีคุณค่าในเชิงพาณิชย์และเก็บเป็นความลับ เช่น สูตรอาหาร กระบวนการ วิธีการผลิต เทคนิค ข้อมูลทางธุรกิจ หรือข้อมูลอื่นๆ ที่มีคุณค่าทางธุรกิจ และองค์กรหรือบุคคลมีความตั้งใจที่จะเก็บเป็นความลับจากผู้อื่น

**ลักษณะของความลับทางการค้า**

1. ข้อมูลที่มีค่าในทางการค้า: ความลับทางการค้าต้องเป็นข้อมูลที่ให้ประโยชน์ทางเศรษฐกิจหรือทางการค้า ซึ่งทำให้ธุรกิจหรือองค์กรที่ครอบครองข้อมูลนี้มีความได้เปรียบทางการแข่งขัน
2. การเก็บรักษาเป็นความลับ: ข้อมูลนี้ต้องถูกเก็บรักษาอย่างเหมาะสม ไม่เปิดเผยต่อสาธารณะ และมีการดำเนินการเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
3. การใช้ประโยชน์อย่างเป็นธรรม: ข้อมูลนี้ต้องมีการใช้งานอย่างถูกต้องและเป็นธรรม โดยไม่ขัดต่อหลักเกณฑ์หรือกฎหมาย

**การคุ้มครองความลับทางการค้า:**

* การนำความลับทางการค้าไปใช้โดยไม่ได้รับอนุญาตเป็นการละเมิดสิทธิทางกฎหมาย
* บ่อยครั้งที่ไม่มีกฎหมายที่ระบุไว้อย่างชัดเจนว่าอะไรคือความลับทางการค้า แต่โดยทั่วไปแล้วความลับทางการค้าจะถูกกำหนดโดยพิจารณาจากปัจจัยหลายประการ เช่น ลักษณะของข้อมูล ความสำคัญทางธุรกิจ และวิธีการรักษาความลับ การพิจารณาเหล่านี้จะแตกต่างกันไปในแต่ละกรณี

1. **สิ่งบ่งชี้ทางภูมิศาสตร์**

* **สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication: GI):** เป็นเครื่องหมายที่ใช้แสดงว่าสินค้าหรือผลิตภัณฑ์นั้นมีแหล่งที่มาจากภูมิภาคหรือท้องถิ่นเฉพาะที่มีชื่อเสียง ซึ่งคุณภาพ ลักษณะเฉพาะ หรือชื่อเสียงของสินค้านั้นๆ เกิดจากภูมิประเทศ สภาพภูมิอากาศ ทรัพยากรธรรมชาติ หรือกระบวนการผลิตเฉพาะที่มีอยู่ในภูมิภาคนั้น
* **ความสำคัญของสิ่งบ่งชี้ทางภูมิศาสตร์:**
* **การคุ้มครองผู้ผลิต:** สิ่งบ่งชี้ทางภูมิศาสตร์ช่วยปกป้องผู้ผลิตในท้องถิ่นจากการที่ผู้อื่นนำชื่อภูมิภาคไปใช้กับผลิตภัณฑ์ที่ไม่ได้มาจากภูมิภาคนั้น
* **การรักษามาตรฐานคุณภาพ:** GI ช่วยส่งเสริมให้ผู้ผลิตรักษามาตรฐานคุณภาพของผลิตภัณฑ์ตามที่กำหนดไว้
* **การส่งเสริมเศรษฐกิจท้องถิ่น:** GI สามารถช่วยเพิ่มมูลค่าให้กับสินค้าท้องถิ่น และเป็นแรงกระตุ้นให้เกิดการพัฒนาเศรษฐกิจในพื้นที่

**ตัวอย่างของสิ่งบ่งชี้ทางภูมิศาสตร์**

ตัวอย่างสิ่งบ่งชี้ทางภูมิศาสตร์ที่มีชื่อเสียงทั่วโลก

* Champagne (แชมเปญ): เป็นไวน์ที่ผลิตในภูมิภาค Champagne ของฝรั่งเศส โดยมีวิธีการผลิตที่เฉพาะเจาะจง ซึ่งทำให้ไวน์นี้มีคุณภาพและรสชาติที่เป็นเอกลักษณ์
* Roquefort (โรเกฟอร์ต): เป็นชีสที่ทำจากนมแกะและมีการบ่มในถ้ำที่เฉพาะเจาะจงในภูมิภาค Roquefort-sur-Soulzon
* Darjeeling Tea (ชาดาร์จีลิง): เป็นชาที่ปลูกในภูมิภาค Darjeeling ของรัฐ West Bengal ของอินเดีย จึงมีรสชาติและกลิ่นหอมเฉพาะตัว
* Scotch Whisky (วิสกี้สก็อตช์): ต้องผลิตในสกอตแลนด์และมีวิธีการผลิตที่เข้มงวดตามกฎหมาย

ตัวอย่างสิ่งบ่งชี้ทางภูมิศาสตร์ในประเทศไทย

* ข้าวหอมมะลิ: ข้าวหอมมะลิเป็นข้าวที่ปลูกในจังหวัดบุรีรัมย์และจังหวัดอื่นๆ ในภาคอีสาน มีความหอมและรสชาติที่เป็นเอกลักษณ์
* กาแฟดอยช้าง: กาแฟที่ปลูกในพื้นที่ดอยช้าง จังหวัดเชียงราย มีรสชาติกลมกล่อมและกลิ่นหอมเฉพาะตัว
* ผ้าทอมือจากเชียงใหม่: ผ้าทอมือที่ผลิตในจังหวัดเชียงใหม่ มีลวดลายและเทคนิคการทอที่เป็นเอกลักษณ์
* น้ำปลาหอยเซลล์: น้ำปลาที่ผลิตจากหอยเซลล์ในจังหวัดประจวบคีรีขันธ์ มีรสชาติที่กลมกล่อมและเป็นที่นิยมในตลาด
* มะพร้าวน้ำหอม: มะพร้าวน้ำหอมที่ปลูกในจังหวัดสมุทรสงคราม มีรสชาติหวานและน้ำมะพร้าวที่หอมสดชื่น ทำให้เป็นที่นิยมในตลาด
* ทุเรียนภูเขาไฟ: ทุเรียนที่ปลูกในจังหวัดสุราษฎร์ธานี มีรสชาติหวานมันและเนื้อแน่น ซึ่งได้รับความนิยมในตลาดทั้งในประเทศและต่างประเทศ

1. **ลิขสิทธ์**

ลิขสิทธิ์ (Copyright)

เป็นสิทธิทางปัญญาประเภทหนึ่งที่ให้ความคุ้มครองผลงานทางวรรณกรรม ศิลปะ และวิทยาศาสตร์ ไม่ว่าจะเป็นในรูปแบบใด เช่น หนังสือ บทความ เพลง ภาพยนตร์ รูปภาพ โปรแกรมคอมพิวเตอร์ เป็นต้น

ลักษณะของลิขสิทธิ์

* สิทธิ์ที่เกิดขึ้นโดยอัตโนมัติ: ลิขสิทธิ์จะเกิดขึ้นทันทีเมื่อผลงานถูกสร้างสรรค์ขึ้น โดยไม่จำเป็นต้องจดทะเบียน
* ความคุ้มครองของลิขสิทธิ์: ลิขสิทธิ์คุ้มครองสิทธิในการทำซ้ำ ดัดแปลง เผยแพร่ แสดงผลงานต่อสาธารณะ และนำผลงานไปใช้ในเชิงพาณิชย์
* ระยะเวลาคุ้มครอง: ลิขสิทธิ์ในประเทศไทยจะคุ้มครองตลอดชีวิตของผู้สร้างสรรค์และต่อเนื่องอีก 50 ปี นับจากวันที่ผู้สร้างสรรค์เสียชีวิต

ความสำคัญของลิขสิทธิ์

* ลิขสิทธิ์เป็นรากฐานสำคัญในการส่งเสริมการสร้างสรรค์นวัตกรรม: ผู้สร้างสรรค์ผลงานต่าง ๆ ไม่ว่าจะเป็นศิลปิน นักประพันธ์ นักประดิษฐ์ เมื่อได้รับการคุ้มครองทางลิขสิทธิ์แล้ว จะมั่นใจได้ว่าผลงานของตนจะไม่ถูกนำไปใช้โดยไม่ได้รับอนุญาต ซึ่งจะกระตุ้นให้เกิดการสร้างสรรค์ผลงานใหม่ ๆ อย่างต่อเนื่อง ทำให้เกิดการพัฒนาทางเศรษฐกิจและสังคม
* ลิขสิทธิ์เป็นเครื่องมือในการคุ้มครองสิทธิของผู้สร้างสรรค์: เมื่อผู้สร้างสรรค์ลงทุนเวลา ความรู้ และทรัพยากรในการสร้างสรรค์ผลงาน การได้รับการคุ้มครองทางลิขสิทธิ์จะทำให้พวกเขาได้รับผลตอบแทนที่เป็นธรรมจากผลงานของตนเอง และเป็นแรงจูงใจให้สร้างสรรค์ผลงานใหม่ ๆ ต่อไป

ผลงานที่ได้รับการคุ้มครองโดยลิขสิทธิ์

* หนังสือ, บทความ, งานเขียน
* เพลง
* ภาพวาด, ภาพถ่าย, ผลงานศิลปะ
* ภาพยนตร์, สารคดี, รายการโทรทัศน์
* โปรแกรมคอมพิวเตอร์และซอฟต์แวร์

**งานที่ได้รับการยกเว้นลิขสิทธิ์**

* 1. งานที่ไม่อยู่ภายใต้การคุ้มครองลิขสิทธิ์
* แนวคิด หลักการ ทฤษฎี หรือกระบวนการ: แนวคิดหรือหลักการทั่วไปไม่ได้รับการคุ้มครองลิขสิทธิ์ เช่น แนวคิดทางวิทยาศาสตร์ ทฤษฎีทางคณิตศาสตร์ เป็นต้น
* ข้อมูลข่าวสารและข้อเท็จจริง: ข้อมูลที่เป็นข้อเท็จจริงหรือข่าวสารทั่วไป เช่น รายงานข่าว ผลการวิจัย หรือข้อมูลทางสถิติกฎหมายและประกาศต่างๆ: กฎหมาย รัฐธรรมนูญ ประกาศ คำสั่ง หรือเอกสารของทางราชการ รวมถึงคำพิพากษาและรายงานของหน่วยงานรัฐ
  1. งานที่สามารถนำมาใช้ได้โดยไม่ถือว่าเป็นการละเมิดลิขสิทธิ์
* การใช้เพื่อการศึกษาและวิจัย: การใช้ผลงานลิขสิทธิ์ในทางวิชาการเพื่อการศึกษา วิจัย หรือวิจารณ์ โดยไม่ใช่ในเชิงพาณิชย์และไม่เกินขอบเขตที่เหมาะสม
* การใช้เพื่อการส่วนตัว: การทำสำเนาผลงานลิขสิทธิ์เพื่อใช้ส่วนตัว เช่น การทำสำเนาเพลงหรือภาพยนตร์เพื่อฟังหรือดูเองที่บ้าน โดยไม่ได้นำไปเผยแพร่ต่อสาธารณะ
* การใช้เพื่อการวิจารณ์หรือการแสดงความคิดเห็น: การอ้างอิงผลงานเพื่อวิจารณ์ แสดงความคิดเห็น หรือเสริมความรู้ในผลงานของผู้อื่น เช่น การรีวิวหนังสือหรือภาพยนตร์
* การใช้ในรายงานข่าว: การนำผลงานลิขสิทธิ์มาใช้ในข่าวสารหรือการรายงานข่าว โดยไม่ใช่การนำผลงานทั้งหมดมาเผยแพร่

**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย**

* ปัจจุบัน ประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ ซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล 7 ฉบับ ดังนี้
* พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2552 ได้มีการเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูล (ฉบับที่ 2) พ.ศ. 2535 และพระราชบัญญัติคุ้มครองข้อมูล (ฉบับที่ 3) พ.ศ. 2542
* พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2553 มีบทบัญญัติโดยตรงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (ฉบับที่ 2) พ.ศ. 2543
* พระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2537 ซึ่งเกี่ยวข้องกับข้อมูล (ฉบับที่ 2) พ.ศ. 2558 และพระราชบัญญัติข้อมูลข่าวสาร (ฉบับที่ 3) พ.ศ. 2558
* พระราชบัญญัติการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ พ.ศ. 2549
* พระราชบัญญัติการค้าอิเล็กทรอนิกส์ พ.ศ. 2546
* พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2546
* พระราชบัญญัติการสื่อสารแห่งชาติ พ.ศ. 2548

**พระราชบัญญัติลิขสิทธิ์ของประเทศไทย**

พระราชบัญญัติลิขสิทธิ์ (Copyright Act) กำหนดกฎเกณฑ์ที่เกี่ยวข้องกับผลงานทางวรรณกรรม ศิลปะ และวิทยาศาสตร์ โดยมีวัตถุประสงค์หลักเพื่อคุ้มครองสิทธิของผู้สร้างสรรค์ผลงาน รวมถึงการส่งเสริมการสร้างสรรค์ผลงานใหม่ๆ ในประเทศไทยโดยมีวัตถุประสงค์ ดังนี้

* คุ้มครองผลงานสร้างสรรค์: ให้สิทธิ์แต่เพียงผู้เดียวแก่ผู้สร้างสรรค์ในการทำซ้ำ ดัดแปลง เผยแพร่ และนำผลงานไปใช้ประโยชน์ในรูปแบบต่างๆ
* ส่งเสริมการสร้างสรรค์: สร้างแรงจูงใจให้เกิดการสร้างสรรค์ผลงานใหม่ๆ ด้วยการรับรองสิทธิ์และผลประโยชน์แก่ผู้สร้างสรรค์
* คุ้มครองสาธารณะ: สร้างความสมดุลระหว่างผลประโยชน์ของผู้สร้างสรรค์และประโยชน์ของสาธารณะในการเข้าถึงและใช้ประโยชน์จากผลงานสร้างสรรค์

**หน่วยงานที่เกี่ยวข้องกับพระราชบัญญัติลิขสิทธิ์**

1. กรมทรัพย์สินทางปัญญา (DIP: Department of Intellectual Property)

* เป็นหน่วยงานหลักในการบริหารจัดการและบังคับใช้กฎหมายลิขสิทธิ์ของประเทศ
* ให้คำปรึกษา ข้อมูล และอำนวยความสะดวกแก่เจ้าของลิขสิทธิ์ ผู้ประกอบการ และประชาชน

1. สำนักงานตำรวจแห่งชาติ

* รับผิดชอบการสืบสวนและจับกุมผู้กระทำความผิดเกี่ยวกับการละเมิดลิขสิทธิ์
* ประสานงานกับกรมทรัพย์สินทางปัญญาในการบังคับใช้กฎหมาย

1. ศาล

* รับผิดชอบการพิจารณาคดีและตัดสินคดีที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์
* ออกคำสั่งและบทลงโทษตามที่กฎหมายกำหนด

1. กระทรวงพาณิชย์

* รับผิดชอบในการกำหนดนโยบายและมาตรการในการคุ้มครองลิขสิทธิ์ในระดับประเทศ
* ประสานงานกับหน่วยงานอื่นๆ ที่เกี่ยวข้อง

**พระราชบัญญัติลิขสิทธิ์ ของประเทศไทย**

พระราชบัญญัติลิขสิทธิ์ของประเทศไทยมีทั้งหมด 5 ฉบับ

* **พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537** – ฉบับหลักที่ใช้ในการคุ้มครองลิขสิทธิ์ในประเทศไทย
* **พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558** – แก้ไขเพิ่มเติมเกี่ยวกับการคุ้มครองลิขสิทธิ์ในยุคดิจิทัลและการจัดการกับการละเมิดลิขสิทธิ์ออนไลน์
* **พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558** – แก้ไขเพิ่มเติมเพื่อเสริมสร้างความคุ้มครองสำหรับงานลิขสิทธิ์ในด้านต่าง ๆ
* **พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 4) พ.ศ. 2564** – แก้ไขเพิ่มเติมเพื่อปรับปรุงกระบวนการบังคับใช้กฎหมายและเพิ่มมาตรการป้องกัน
* **พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 5) พ.ศ. 2565** – แก้ไขเพิ่มเติมล่าสุดที่มุ่งเน้นการคุ้มครองลิขสิทธิ์ในบริบทของเทคโนโลยีและดิจิทัล

เพื่อป้องกันไม่ให้ละเมิด พ.ร.บ. ขออนุญาต, ให้เครดิต, ห้ามดัดแปลง ทำซ้ำ

**ลักษณะทั่วไปของลิขสิทธิ์**

ผู้ที่สร้างสรรค์งานจะเป็นผู้ถือสิทธิลิขสิทธิ์ โดยมีลักษณะดังนี้

* ลิขสิทธิ์เป็นสิทธิแต่ผู้เดียว (exclusive rights)
* ลิขสิทธิ์เป็นสิทธิในทางทรัพย์สิน (property rights)
* ลิขสิทธิ์เป็นสิทธิที่มีการจำกัดเวลา
* ลิขสิทธิ์เป็นสิทธิสากล (multiple rights)
* ลิขสิทธิ์แยกต่างหากจากการกรรมสิทธิ์ (independence of ownership)

**การได้มาซึ่งลิขสิทธิ์**  
สิทธิในลิขสิทธิ์จะเกิดขึ้นโดยทันทีนับตั้งแต่ผู้สร้างสรรค์ได้สร้างผลงานโดยไม่ต้องจดทะเบียน ซึ่งมีลักษณะการได้มาดังนี้

* คุ้มครองทันทีที่ได้มีการสร้างสรรค์งานนั้น
* กรณีที่ยังไม่ได้มีการโฆษณางาน ผู้สร้างสรรค์ต้องเป็นผู้มีสัญชาติไทยหรือมีสัญชาติในประเทศที่เป็นภาคีแห่งอนุสัญญา ว่าด้วยการคุ้มครองลิขสิทธิ์ที่ประเทศไทยเป็นภาคีอยู่ด้วย
* กรณีที่มีการโฆษณางานแล้ว ต้องเป็นการโฆษณาครั้งแรกได้ทำขึ้นในราชอาณาจักรหรือในประเทศที่เป็นภาคีฯ
* กรณีที่ผู้สร้างสรรค์เป็นนิติบุคคล ต้องเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

**สิทธิของเจ้าของลิขสิทธิ์**  
เจ้าของลิขสิทธิ์ย่อมมีสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ ต่องานอันมีลิขสิทธิ์ของตน ดังต่อไปนี้

* มีสิทธิ์ในการทำซ้ำ ดัดแปลง จำหน่าย ให้เช่า คัดลอก เลียนแบบทำสำเนา
* การทำให้ปรากฏต่อสาธารณชนหรืออนุญาตให้ผู้อื่นใช้สิทธิของตน โดยมีหรือไม่มีค่าตอบแทนก็ได้

**อายุการคุ้มครองลิขสิทธิ์**

* งานทั่วไป ลิขสิทธิ์จะมีตลอดอายุผู้สร้างสรรค์ และจะมีต่อไปอีก 50 ปี นับแต่ผู้สร้างสรรค์ถึงแก่ความตาย กรณีเป็นนิติบุคคล ลิขสิทธิ์จะมีอยู่ 50 ปี นับแต่ได้สร้างสรรค์งานนั้นขึ้น
* งานภาพถ่าย โสตทัศนวัสดุ ภาพยนตร์ หรืองานแพร่เสียง แพร่ภาพ ลิขสิทธิ์มีอยู่ 50 ปี นับแต่ได้สร้างสรรค์งานนั้นขึ้น  
  ผลภายหลังลิขสิทธิ์หมดอายุ  
  งานนั้นตกเป็นสมบัติของสาธารณะ บุคคลใดๆ สามารถใช้งานนั้นๆ ได้โดยไม่เป็นการละเมิดลิขสิทธิ์

**รูปแบบการละเมิดทรัพย์สินทางปัญญา**

* 1. การปลอมแปลง เป็นการผลิตที่มีการใช้วัสดุ รูปลักษณ์ ตราสินค้าที่เหมือนกับของเจ้าของทุกประการโดยที่ผู้ซื้ออาจแยกไม่ออกว่าเป็นของจริงหรือไม่ ดังที่เราพบเห็นกันใน ท้องตลาด เช่นการปลอม นาฬิกาโรเล็กซ์ เสื้อโปโล กระเป๋าหลุยส์ วิตตอง สินค้าของ Dior เป็นต้น
  2. การลอกเลียนแบบ โดยที่ตัวสินค้ามีรูปร่างหน้าตาเหมือนสินค้าของเจ้าของผู้ผลิตแต่มีการปรับเครื่องหมายการค้าเล็กน้อย เช่น PRADA เป็น PRADO , Sony เป็น Somy เป็นต้น
  3. การลักลอบผลิต คือการลักลอบผลิต เทปผี ซีดีเถื่อน ซึ่งเราได้พบเห็นข่าวการลักลอบผลิตอยู่เป็นประจำ เช่น ซีดีภาพยนตร์เรื่องต้มยำกุ้ง ในอดีต

**บทลงโทษการละเมิดลิขสิทธิ์ ใน พ.ร.บ.ลิขสิทธิ์**

1. การละเมิดลิขสิทธิ์ทั่วไป  
   โทษปรับตั้งแต่ 20,000 บาท ถึง 200,000 บาท
2. 2.การละเมิดลิขสิทธิ์เพื่อการค้า  
   ﻿﻿โทษจำคุกตั้งแต่ 6 เดือน ถึง 4 ปี หรือปรับตั้งแต่ 100,000 บาท ถึง 800,000 บาท หรือทั้งจำทั้งปรับ
3. 3.การจำหน่ายสินค้าละเมิดลิขสิทธิ์เพื่อหากำไรทางการค้า  
   ﻿﻿โทษจำคุกตั้งแต่ 3 เดือน ถึง 2 ปี หรือปรับตั้งแต่ 50,000 บาทถึง 400,000 บาท หรือทั้งจำทั้งปรับ

การละเมิดลิขสิทธิ์ถือเป็นความผิดอาญา และผู้เสียหายสามารถแจ้งความร้องทุกข์เพื่อดำเนินคดีได้ โดยกฎหมายยังระบุว่าการละเมิดลิขสิทธิ์นั้นไม่สามารถยอมความได้ ซึ่งหมายความว่าผู้กระทำผิดจะต้องรับโทษตามกฎหมาย

﻿﻿**Business Software Alliance (BSA)** หรือในชื่อเต็มคือ BSA | The Software Alliance

* สมาคมการค้าระดับโลกที่ก่อตั้งขึ้นโดยมีวัตถุประสงค์หลักในการคุ้มครองลิขสิทธิ์ซอฟต์แวร์ของบริษัทสมาชิกและต่อสู้กับการละเมิดลิขสิทธิ์ซอฟต์แวร์ทั่วโลก มีสมาชิกมากกว่า 1,000 รายจากกว่า 70 ประเทศทั่วโลก โดยสมาชิกส่วนใหญ่เป็นบริษัทซอฟต์แวร์รายใหญj
* ภารกิจหลักของ BSA
* การสนับสนุนกฎหมาย: มีบทบาทในการผลักดันกฎหมายที่คุ้มครองสิทธิ์ทางปัญญาและส่งเสริมการปฏิบัติตามกฎหมาย ลิขสิทธิ์ในหลายประเทศทั่วโลก
* การบังคับใช้กฎหมาย: ดำเนินการทางกฎหมายต่อผู้ที่ละเมิดลิขสิทธิ์ซอฟต์แวร์ โดยเฉพาะการใช้ซอฟต์แวร์เถื่อนในองค์กร ธุรกิจ ซึ่งรวมถึงการสืบสวน การดำเนินคดี และการเรียกร้องค่าเสียหาย
* การให้ความรู้ มุ่งเน้นการให้ความรู้และสร้างความตระหนักเกี่ยวกับความสำคัญของการใช้ซอฟต์แวร์ถูกลิขสิทธิ์ทั้งในองค์กรและบุคคลทั่วไป

**ข้อปฏิบัติตาม พ.ร.บ.ลิขสิทธิ์ พ.ศ. 2537 และฉบับที่ 2 พ.ศ. 2558**

**การคัดลอกเนื้อหาบนหน้าเว็บ มาวางในมาโพสต์ทาง Facebook หรือเว็บเราละเมิดลิขสิทธิ์หรือไม่?**

* ขึ้นอยู่กับลักษณะและเงื่อนไขของเนื้อหานั้นๆ บางกรณีที่การใช้งานอาจถือว่าเป็นการใช้งานที่ยุติธรรมหรือการใช้งานที่ไม่ต้องได้รับอนุญาต (fair use) เช่น การใช้เพื่อการศึกษา การวิจัยหรือการวิจารณ์
* ถ้าเป็นรายบุคคล เป็น Facebook ใช้ส่วนตัว สามารถใช้ได้ ทั้งนี้ต้อง อ้างอิงแหล่งที่มา ใช้ส่วนตัว และ ไม่มีแสวงหาผลกำไร ถึงจะไม่ผิดลิขสิทธิ์
* แต่ถ้าในกรณีนิติบุคคล ถือว่าไม่ได้ ถ้าเว็บไซต์คุณมีแบนเนอร์โฆษณา หรือ Facebook มีกิจกรรมทางธุรกิจ ถือว่าเข้าข่ายผิดลิขสิทธิ์

﻿﻿**ถ้าเว็บไซต์ หรือ blog ของเรา นำ embed วีดีโอจาก YouTube แปะใส่ในหน้าเว็บเรา ทำได้ไหม ผิดหรือเปล่า?**

* ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 มาตรา 15 ระบุว่า เจ้าของลิขสิทธิ์มีสิทธิทำการเผยแพร่ต่อสาธารณชน โดยวิธีการใดๆ ก็ได้ เว้นแต่มีกฎหมายบัญญัติไว้เป็นอย่างอื่น
* การฝังโค้ด (embed) วิดีโอจาก YouTube เป็นการเผยแพร่ต่อสาธารณชนโดยวิธีการหนึ่ง โดยเจ้าของ วิดีโอใน YouTube อนุญาตให้ผู้ที่เป็นเจ้าของเว็บไซต์หรือบล็อกสามารถนำวิดีโอไปฝังในเว็บไซต์หรือบล็อกของตนได้ โดยเจ้าของวิดีโอจะได้รับค่าตอบแทนจาก YouTube อยู่แล้ว
* เมื่อฝังวิดีโอ แต่ไม่ได้ทำสำเนาหรือเปลี่ยนแปลงเนื้อหา แต่เพียงแค่สร้างลิงก็ไปยังเนื้อหาที่อยู่บน  
  YouTube

﻿﻿**หากต้องการนำคลิป YouTube ไปใช้ควรทำอย่างไร?**

* ต้องเผยชื่อ user YouTube เจ้าของคลิปนั้น เพื่ออ้างอิง และคลิปที่ใช้ได้ต้องเผยแพร่แบบ  
  สาธารณะ
* ถ้าเป็นคลิป YouTube แบบ Private หรือแชร์ลิงค์เฉยๆ ที่ไม่ใช่สาธารณะนำมาใช้ ถือว่าผิดลิขสิทธิ์
* กรณีแฟนเพจ Facebook แชร์ภาพของ Fan Page อื่น เพื่อเรียกเรตติ้ง มีความเสี่ยงถูกฟ้อง เพราะเรื่องแสวงหาผลกำไร

﻿﻿**ถ้าแปลจากเว็บต่างประเทศ แล้วอ้างอิงให้แล้ว ผิดลิขสิทธิ์หรือไม่?**

* ถ้าเป็นเนื้อหาข่าว ไม่ผิดลิขสิทธิ์ แต่ถ้าเป็นบทความอาจผิดลิขสิทธิ์ได้ ถ้าใช้ในเรื่องแสวงหาผลกำไร หรือใช้ในเชิงพาณิชย์ ทั้งนี้ การนำเนื้อหามารีไรท์เรียบเรียงใหม่ ถือว่าไม่ผิด แต่ถ้า copy paste แปลรายคำ ถือว่าผิดลิขสิทธิ์
* ตัวอย่างเนื้อหาข่าวที่ไม่ผิดลิขสิทธิ์ เช่น เนื้อหาข่าวว่าเกิดอะไรขึ้น ข้อมูลทั่วไป ราคาหุ้น พยากรณ์อากาศหนังฉายวันนี้ ราคาน้ำมัน ผลการแข่งขันฟุตบอล อันนี้ไม่เป็นลิขสิทธิ์ สามารถแชร์ หรือใช้ไดh
* แต่ถ้าเป็น พวกภาพข่าว รูป บทสัมภาษณ์ข่าว คอลัมน์ข่าว ถือว่าเป็นลิขสิทธิ์ หากนำไปใช้โดยไม่ขออนุญาตเจ้าของภาพ หรือเจ้าของคอลัมน์ อาจเสี่ยงถูกฟ้องในข้อหาละเมิดลิขสิทธิ์ได

**มาตรการป้องกันทางเทคโนโลยี**(Technological Protection Mesures: TPMs)  
เจ้าของลิขสิทธิ์นำมาตรการต่างๆ มาใช้เพื่อป้องกันการละเมิดลิขสิทธิ์ โดยแบ่งได้เป็น 2 ประเภท คือ

1. มาตรการทางสัญญา จำกัดสิทธิต่างๆ เพื่อควบคุมการใช้งานอันมีลิขสิทธิ์โดยผ่านสัญญาในรูปแบบต่างๆ  
   เช่น Shrink-wrap License, Click-wrap License
2. มาตรการทางเทคโนโลยี โดยนำเอาเทคโนโลยีมาใช้เพื่อป้องกันการละเมิดลิขสิทธิ์ เช่น เจ้าของลิขสิทธิ์ใน สิ่งบันทึกเสียงอาจผลิตซีดีเพลงออกจำหน่ายโดยใช้ เทคโนโลยีป้องกันมิให้มีการทำสำเนางาน หรือเจ้าของ ลิขสิทธิ์ในงานวรรณกรรมนำเอางานนั้นบันทึกลงในแผ่นซีดี โดยกำหนดว่าผู้ใช้สามารถอ่านหนังสือจากซีดีดังกล่าวได้ไม่เกินระยะเวลาหรือจำนวนครั้งที่กำหนดเท่านั้น

**ข้อมูลการบริหารสิทธิ์** (Rights Management Information)  
﻿﻿"ข้อมูลบริหารสิทธิ" ในทางปฏิบัติหมายถึง สิทธิในการประกาศ ตัวเองเป็นเจ้าของลิขสิทธิ์ของเจ้าของ ลิขสิทธิ์ตัวอย่างข้อมูลบริหารสิทธิ เช่น ลายเซ็น ลายน้ำ ลายเซ็น ชื่อไฟล์ เป็นต้น  
﻿﻿และการละเมิดคือการไปแก้ไขข้อมูลต่างๆ ที่ติดมากับตัวงาน การนำลายเซ็นหรือลายน้ำออกจากรูปภาพ ไปจนถึงการแก้ไข/เปลี่ยนชื่อไฟล์ไปจนถึงเมทาเดตา (metadata) ของไฟล์ ก็อาจจะถือเป็นการละเมิดข้อมูลบริหารสิทธิด้วย

**เพิ่มข้อยกเว้นการละเมิดลิขสิทธิ์**

* หลักการระงับไปซึ่งสิทธิ (Ehaustion of Rights) การจำหน่ายต้นฉบับหรือสำเนางานอันมีลิขสิทธิ์โดยผู้ได้มาซึ่งกรรมสิทธิ์ในต้นฉบับหรือสำเนางานอันมีลิขสิทธิ์นั้นโดยชอบด้วยกฎหมาย มิให้ถือว่าเป็นการละเมิดลิขสิทธิ์
* การทำซ้ำชั่วคราว (Temporary Copy) การกระทำแก่งานอันมีลิขสิทธิ์ที่ทำหรือได้มาโดยชอบด้วยกฎหมายในระบบคอมพิวเตอร์ที่มีลักษณะเป็นการทำซ้ำที่จำเป็นต้องมีสำหรับการนำสำเนามาใช้เพื่อให้อุปกรณ์ที่ใช้ในระบบคอมพิวเตอร์หรือกระบวนการส่งงานอันมีลิขสิทธิ์ทางระบคอมพิวเตอร์ทำงานได้ตามปกติ มิให้ถือว่าเป็นการละเมิดลิขสิทธิ์

**การทำซ้ำและการเชื่อมโยงงานลิขสิทธิ์บนอินเทอร์เน็ต  
ด้วยวิธี Hyperlink และ Embedded (Deep Link)**

* การสร้างสิ้งค์เพื่อเชื่อมโยงไปยังเว็บไซต์อื่นนั้นไม่น่าจะเป็นความผิดตามกฎหมายลิขสิทธิ์ได้ เพราะการกระทำเช่นนี้ไม่ได้เป็นการทำซ้ำงานอันมีลิขสิทธิ์ของเจ้าของเว็บไซต์อื่นมาไว้ที่เว็บไซต์ของผู้กระทำแต่อย่างใด
* หากมีการเชื่อมโยงข้อมูลโดยนำงานบางส่วนของงานอันมีลิขสิทธิ์อื่นมา ใส่ไว้ในเว็บเพจ ที่เชื่อมโยงข้อมูล โดยมีการอ้างอิงแหล่งที่มาไว้ การเชื่อมโยง ข้อมูลเช่นนี้อาจเปรียบเทียบได้กับการอ้างอิง (Reference) งานอันมีลิขสิทธิ์ ของผู้อื่นทำนองเดียวกัน กับการที่ผู้แต่งหนังสือเรื่องหนึ่งอ้างอิงหนังสือ ของผู้อื่น ซึ่งถือว่าเป็นข้อยกเว้นของการละเมิดลิขสิทธิ์

**กรณี YouTube กับการป้องกันด้านลิขสิทธิ์**  
YouTube มีมาตรการป้องกันด้านลิขสิทธิ์ที่เข้มงวด เพื่อป้องกันการละเมิดลิขสิทธิ์และเพื่อคุ้มครองสิทธิ์ของเจ้าของเนื้อหาที่อับโหลดหรือเยแพร่บนแพลตฟอร์ม โดยมีเครื่องมือและกระบวนการสำคัญที่ใช้ในการจัดการปัญหาด้าน ลิขสิทธิ์ ดังนี้

1. Content ID: ระบบที่ตรวจสอบและจับคู่เนื้อหาที่อับโหลดกับฐานข้อมูลเนื้อหาที่มีลิขสิทธิ์ หากพบการละเมิดเจ้าของลิขสิทธิ์สามารถเลือกบล็อกเนื้อหา เก็บรายได้ หรือดูสถิติการใช้งานได้
2. Copyright Strike: หากพบการละเมิดลิขสิทธิ์ ผู้ใช้อาจได้รับการแจ้งเตือน (Strike) และหากได้รับ Strike 3 ครั้งใน 90 วัน ช่องอาจถูกปิดอย่างถาวร
3. การคัดค้านและแก้ไข: ผู้ใช้สามารถคัดค้านการแจ้งเตือนหรือลบ/แก้ไขเนื้อหาที่ละเมิดลิขสิทธิ์ได้
4. การให้ความรู้: YouTube ให้คำแนะนำเกี่ยวกับลิขสิทธิ์แก่ผู้ใช้เพื่อป้องกันการละเมิด
5. ความร่วมมือกับเจ้าของลิขสิทธิ์: YouTube ทำงานร่วมกับเจ้าของลิขสิทธิ์เพื่อปกป้องสิทธิ์ของพวกเขาและคุ้มครองเนื้อหาบนแพลตฟอร์ม

กิจกรรมของการใช้เทคโนโลยีสารสนเทศที่เกี่ยวกับงานที่ได้รับการคุ้มครองทรัพย์สินทางปัญญา

1. การสร้างและเผยแพร่เนื้อหาออนไลน์

การเขียนบทความและ Blog : การสร้างเนื้อหาที่เป็นบทความหรือบล็อกที่มีลิขสิทธิ์ ซึ่งผู้เขียนจะมีสิทธิ์ในการคุ้มครองเนื้อหาที่สร้างขึ้น

การผลิตวิดีโอและสือมัลติมีเดีย: การสร้างวิดีโอ คลิปเสียง หรือภาพเคลื่อนไหวที่ถูกเผยแพร่ผ่านแพลตฟอร์มออนไลน์ เช่น YouTube ซึ่งเนื้อหา

การพัฒนาเว็บไซต์และซอฟต์แวร์: การออกแบบเว็บไซต์หรือพัฒนาโปรแกรมคอมพิวเตอร์ที่มีการคุ้มครองทรัพย์สินทางปัญญาภายใต้กฎหมาย

1. การจัดการและการป้องกันทรัพย์สินทางปัญญา

การใช้ระบบป้องกันลิขสิทธิ์ (Digital Rights Management - DRM): การใช้เทคโนโลยีเพื่อป้องกันการทำสำเนาหรือการเข้าถึงเนื้อหาที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต เช่น การใช้รหัสผ่านหรือการเข้ารหัสไฟล์

การใช้ระบบ Content ID: แพลตฟอร์มออนไลน์ เช่น YouTube ใช้ระบบ Content ID เพื่อตรวจจับและจัดการกับการละเมิดลิขสิทธิ์โดย อัตโนมัติ

1. การเข้าถึงและการใช้งานเนื้อหาที่มีลิขสิทธิ์

การดาวน์โหลดเพลง ภาพยนตร์ และซอฟต์แวร์: การซื้อและดาวน์โหลดเนื้อหาที่มีลิขสิทธิ์จากร้านค้าออนไลน์ เช่น iTunes, Google Play หรือ Amazon ซึ่งผู้ใช้จะได้รับสิทธิ์ในการใช้งานเนื้อหาภายใต้ข้อตกลงที่กำหนด

การสตรีมมิ่ง (Streaming): การรับชมวิดีโอหรือฟังเพลงผ่านแพลตฟอร์มสตรีมมิ่ง เช่น Netfix, Spotify ซึ่งผู้ให้บริการและผู้ใช้ต้องปฏิบัติตามกฎหมายลิขสิทธิ

1. การศึกษาและวิจัย

การใช้ทรัพยากรออนไลน์เพื่อการศึกษา: การใช้บทความทางวิชาการ หนังสือดิจิทัล หรือฐานข้อมูลออนไลน์ที่มีลิขสิทธิ์ในงานวิจัยหรืองานเขียนทางวิชาการ โดยปฏิบัติตามข้อตกลงการใช้งานที่กฎหมายลิขสิทธิ์กำหนด

การพัฒนาและเผยแพร่งานวิจัย: การเผยแพร่งานวิจัยหรือบทความทางวิชาการผ่านเว็บไซต์ของสถาบันการศึกษา หรือวารสารออนไลน์ที่มีการ คุ้มครองทรัพย์สินทางปัญญา

1. การค้าขายและการตลาดดิจิทัล

การขายสินค้าออนไลน์ที่มีลิขสิทธิ์: การขายหนังสือ เพลง หรือผลิตภัณฑ์ดิจิทัลอื่น ๆ ที่ได้รับการคุ้มครองทรัพย์สินทางปัญญาผ่านแพลตฟอร์มออนไลน

การใช้แบรนด์และเครื่องหมายการค้า: การสร้างและใช้แบรนด์หรือเครื่องหมายการค้าในสื่อดิจิทัล เช่น เว็บไซต์ โซเชียลมีเดีย หรือโฆษณาออนไลน์ ซึ่งได้รับการคุ้มครองภายใต้กฎหมายเครื่องหมายการค้า

1. การใช้และพัฒนาซอฟต์แวร์

การพัฒนาและจำหน่ายซอฟต์แวร์: ผู้พัฒนาซอฟต์แวร์มีสิทธิ์ตามกฎหมายลิขสิทธิ์ในการคุ้มครองโค้ดและการออกแบบซอฟต์แวร์ และสามารถจำหน่ายซอฟต์แวร์นันในรูปแบบที่ได้รับการคุ้มครอง

การใช้ซอฟต์แวร์ที่ได้รับอนุญาต: ผู้ใช้สามารถใช้ซอฟต์แวร์ตามเงื่อนไขการอนุญาต (license) ที่กำหนด โดยการใช้ซอฟต์แวร์ที่ไม่มีใบอนุญาต ถือว่าเป็นการละเมิดลิขสิทธิ์

**การใช้งานอันมีลิขสิทธิ์ของผู้อื่นโดยไม่ละเมิดลิขสิทธ์**

* 1. งานอันมีลิขสิทธิ์และเหตุผลในการคุ้มครอง : ประโยชน์สาธารณะ เพื่อให้ทุกคนหรือสาธารณะสามารถเข้าถึงและเข้าใช้งานลิขสิทธิ์ได้ภายในขอบเขตที่เหมาะสม
  2. สิทธิ์แต่ผู้เดียวของเจ้าของลิขสิทธิ์ : ผู้ที่ต้องการใช้งานอันมีลิขสิทธิ์แต่ละชิ้นจึงควรต้องติดต่อเพื่อขออนุญาตจากเจ้าของลิขสิทธิ์ก่อนการใช้งาน
  3. ประเภทการใช้งานอันมีลิขสิทธิ์  
     3.1 การขออนุญาตใช้ลิขสิทธิ์  
     3.2 การใช้งานลิขสิทธิ์อย่างเป็นธรรม หรือที่เรียกว่า "fair use"
  4. การใช้งานที่เป็น public domain /"สมบัติสาธารณะ" แบ่งได้เป็น 3 กลุ่มใหญ่คือ

สิ่งที่ไม่เป็นงานลิขสิทธิ์

งานที่เจ้าของลิขสิทธิ์สละลิขสิทธิ์

งานที่สิ้นอายุการคุ้มครองลิขสิทธิ์

**ครีเอทีฟคอมมอนส์**

* แนวคิดของ Creative Commons  
  เป็นสัญญาอนุญาตทางลิขสิทธิ์ประเภทหนึ่งพัฒนาโดย Hewlett Foundation study องค์กรไม่แสวงกำไรองค์กรหนึ่งที่เน้นงานด้านกฎหมาย
* วัตถุประสงค์ของสัญญานี้เพื่อให้เจ้าของผลงานอันมีลิขสิทธิ์สามารถแสดงข้อความอันอำนวยความสะดวกให้สาธารณชนรู้ถึงสิทธิ์ในผลงาน และทราบว่าจะนำงานอันมีลิขสิทธ์ของตนไปใช้ได้โดยไม่ต้องขออนุญาตและไม่ถือว่าเป็นการละเมิดลิขสิทธิ์ โดยผู้ที่นำผลงานไปใช้ต้องปฏิบัติตามเงื่อนไขที่กำหนด

**Creative Commons licenses**

* "สัญญาอนุญาตให้ใช้สิทธิของครีเอทีฟคอมมอนส์" สัญญาอนุญาตให้ใช้สิทธิ "3 ชั้น" ของครีเอทีฟคอมมอนส์
* ครีเอทีฟคอมมอนส์ ไม่ได้เป็นสัญญาที่มีไว้เพื่อ ผลทางกฎหมายเหมือนสัญญาทั่วไป แต่เป็นแบบสัญญาที่ถูกออกแบบให้สื่อความหมายได้ทั้งในด้านของกฎหมาย ด้านของผู้ใช้งานและด้านของเครื่อง
* ครีเอทีฟคอมมอนส์เป็นทางเลือกหรือกรอบใหม่ในการคุ้มครองลิขสิทธิ์ เป็นทางเลือกเพื่อเปิดโอกาสให้มีการแบ่งปันข้อมูลกันได้สะดวกมาก โดยเป็นทางเลือกที่ไม่ติดยึดกับกรอบของลิขสิทธิ์ที่กำหนดให้ "ทุกอย่างทำไม่ได้"จนกว่าจะได้รับอนุญาตก่อน
* สำหรับครีเอทีฟคอมมอนส์ ก็ไม่ได้เปิดกว้างไปทุกส่วน แต่ให้ใช้งานลิขสิทธิ์ทุกอย่างได้โดยไม่ต้องขออนุญาต แต่ได้เสนอทางออกที่ตำนึงถึงความสมดุลโดยเปิดทางเลือกให้ผู้สร้างสรรค์แต่ละคนเลือกเองว่าจะยอมอนุญาตแค่ไหนและในงานชิ้นใด

**สัญญาอนุญาตให้ใช้สิทธิ "3 ชั้น"**  
**"ชั้นที่หนึ่ง"** เป็นชั้นที่แสดงสิทธิหน้าที่ใน กรอบของกฎหมาย ซึ่งอธิบายเป็นภาษากฎหมายอย่างที่นักกฎหมายใช้กันทั่วไป โดยอาจเรียกชั้นที่หนึ่งนี้ว่า เป็นชั้นของ  
ความหมายทางกฎหมาย  
**"ชั้นที่สอง"** เป็นชั้นที่เขียนไว้ให้ผู้ใช้งานที่ ไม่ต้องเป็นนักกฎหมายอ่าน เป็นสัญญา ของคน ทั่วไป ซึ่งมีไว้ให้ทั้งผู้อนุญาตให้ใช้ งานและผู้ใช้งานสามารถเข้าใจตรงกัน ทั้ง ส่วนของสาระสำคัญและเงื่อนไขต่างๆ ของ แบบสัญญา ชั้นที่สองนี้ทำให้สิทธิหน้าที่ ตามกฎหมายอยู่ในรูปที่อ่านและเข้าใจง่าย แม้ว่าโดยรูปแบบของชั้นที่สองไม่สามารถ ทำให้เกิดการอนุญาตให้ใช้สิทธิและเกิดผล ทางกฎหมายโดยตัวเอง  
**"ชั้นที่สาม"** เป็นชั้นที่ทำให้เครื่องและ ซอฟต์แวร์ต่างๆ อ่านและเข้าใจแบบสัญญา อนุญาตให้ใช้สิทธิได้ซึ่งประกอบด้วย สาระสำคัญของการอนุญาตและสิทธิหน้าที่ ต่างๆ ในสัญญา วิธีการอธิบายให้เครื่องเข้าใจตามที่กล่าว เป็นข้อมูลที่อยู่ในรูปแบบของโค้ดหรือเมตาดาต้า ที่สามารถถูกอ่านและประมวลผลโดยเครื่องจักรหรือซอฟต์แวร์ มาถูกพัฒนาออกเป็นภาษาที่เรียกว่า CC Rights Expression Language หรือ CC RELมีเมนูบริบท

สัญลักษณ์ของสัญญาอนุญาตให้ใช้สิทธิของครีเอทีฟคอมมอนส์

﻿﻿แสดงที่มา/อ้างที่มา (Atribution - BY) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าว และสร้างงานดัดแปล่งจากชิ้นงานดังกล่าว ได้เฉพาะกรณีที่ผู้นั้นได้แสดงเครดิตของผู้เขียนหรือผู้ให้อนุญาตตามที่ระบุไว้



﻿﻿﻿﻿ไม่ใช้เพื่อการค้า (NonCommercial - NC) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าว และสร้างงานดัดแปลงจากชิ้นงานดังกล่าว ได้เฉพาะกรณีที่ไม่นำไปใช้ในทางการค้าผู้ให้อนุญาตตามที่ระบุไว้

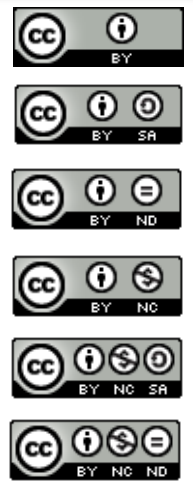


﻿﻿﻿﻿ไม่ดัดแปลง (No Derivative Works -ND) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าวในรูปแบบที่ไม่ถูกดัดแปลงเท่านั้น



﻿﻿﻿﻿อนุญาตแบบเดียวกัน (Share Alike - SA) : อนุญาตให้ผู้อื่นแจกจ่ายงานดัดแปลง เปลี่ยนรูปหรือต่อเติมงานได้เฉพาะกรณีที่ชิ้นงานดัดแปลงนั้นเผยแพร่ด้วยสัญญาอนุญาตที่เหมือนกันทุกประการกับงานต้นฉบับ หรือสรุปง่ายๆ ว่าต้องใช้สัญญาอนุญาตชนิดเดียวกันกับงานดัดแปลง ต่อยอดผู้ให้อนุญาตตามที่ระบุไว้

Attribution : CC BY  
ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มา  
Attribution CC - BY -SA ให้เผยแพร่ ดัดแปลง โดยต้องระบุ ที่มาและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตเดียวกัน  
Attribution CC - BY -ND  
ให้เผยแพร่ โดยต้องระบุที่มา แต่ห้ามดัดแปลง  
Attribution CC- BY -NC  
ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ ห้ามใช้เพื่อการค้า  
Attribution CC- BY - NC - SA  
ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ห้ามใช้เพื่อการค้าและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตชนิดเดียวกัน  
Attribution CC- BY - NC -ND  
ให้เผยแพร่ โดยต้องระบุที่มาแต่ห้ามดัดแปลงและห้ามใช้เพื่อการค้า



**CC กับ ซอฟต์แวร์และฮาร์ดแวร์**

* สัญญาอนุญาตให้ใช้สิทธิของครีเอทีฟคอมมอนส์สามารถใช้ได้กับงานทุกชนิดที่ยังได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์ เช่น ข้อมูลการศึกษา ดนตรี ภาพถ่าย ฐานข้อมูลเป็นต้น แต่งานประเภทเดียวที่ครีเอทีฟคอมมอนส์ไม่แนะนำให้ใช้แบบของสัญญาอนุญาตให้ใช้สิทธิที่กล่าวมาคือ "คอมพิวเตอร์ซอฟต์แวร์และฮาร์ดแวร์
* โดยแนะนำว่าควรใช้แบบสัญญาอนุญาตให้ใช้สิทธิที่ออกแบบเฉพาะสำหรับซอฟต์แวร์แทน ยกตัวอย่างเช่นแบบสัญญาของ Free Software Foundation หรืออาจระบุให้งานซอฟต์แวร์นั้นเป็นโอเพนซอร์ซ (open  
  source) ในกรอบของ Open Source Initiative
* เพราะ สัญญาอนุญาตให้ใช้สิทธิของครีเอทีฟคอมมอนส์ในปัจจุบันยังไม่เชื่อมต่อกับ GNU General Public License (GPL) ซึ่งเป็นฐานข้อมูลสำคัญของ
* ฟรีซอฟต์แวร์หรือซอฟต์แวร์เสรี ที่ให้ผู้ใช้ซอฟต์แวร์มีเสรีภาพในการใช้งาน ศึกษาจำหน่ายจ่ายแจก รวมทั้งปรับปรุงและเปิดให้คนทั่วไปใช้งานและพัฒนาต่อไป

**สัญญาอนุญาตที่เกี่ยวกับผลิตภัณฑ์ซอฟต์แวร์**

* ﻿﻿กรอบของกฎหมายที่กำหนดวิธีการใช้งานและการแจกจ่ายซอฟต์แวร์ โดยจะกำหนดว่าซอฟต์แวร์สามารถถูกใช้งาน แก้ไข และแจกจ่ายได้อย่างไร และมักจะแยกความแตกต่างระหว่างการใช้งานส่วน บุคคล ทางการค้า และแบบโอเพนซอร์ส (Open Source)
* มีวัตถุประสงค์เพื่อใช้เพื่อคุ้มครองซอฟต์แวร์และควบคุมการใช้งานหรือการเผยแพร่ซอฟต์แวร์ ไม่ให้เกิดการละเมิดลิขสิทธิ์
* เป็นเอกสารในทางกฎหมาย โดยจะอยู่ในรูปของเอกสารหรือแบบอิเล็กทรอนิกส์ก็ได้ อาจจะเรียกว่า สัญญาอนุญาตใช้ซอฟต์แวร์ หรือใบอนุญาตซอฟต์แวร์ (Software License/Licence)

**ประเภทของสัญญาอนุญาตซอฟต์แวร์**

สัญญาอนุญาตซอฟต์แวร์ (Software License) มีหลายประเภท โดยทั่วไปแบ่งออกเป็นสองประเภทหลัก คือ

1. สัญญาแบบปิด (Proprietary License) เป็นสัญญาที่ผู้ใช้จะได้รับสิทธิ์ในการใช้ซอฟต์แวร์แต่เพียงผู้เดียว แต่ไม่สามารถดัดแปลงหรือแจกจ่ายต่อได้

2. สัญญาอนุญาตแบบเปิด (Open Source License) เป็นสัญญาอนุญาตที่ผู้ใช้สามารถดัดแปลงและแจกจ่ายซอฟต์แวร์ต่อได้ โดยมีหลายประเภทย่อย เช่น MIT License, Apache License, GNU General Public License (GPL), และอื่น ๆ  
แต่ละประเภทของสัญญาอนุญาตมีข้อจำกัดและสิทธิ์ที่แตกต่างกัน ดังนั้นควรทำความเข้าใจในเงื่อนไขและ ข้อกำหนดของสัญญาอนุญาตก่อนการใช้งาน

**ประเภทของสัญญาอนุญาตซอฟต์แวร์**  
**1. สัญญาอนุญาตแบบปิด หรือแบบกรรมสิทธิ์ หรือ ซอฟต์แวร์จำกัดสิทธิ์ (proprietary software)** ซอฟต์แวร์ที่สิทธิ์ในการใช้งาน ทำซำ ดัดแปลง หรือ เผยแพร่ ถูกจำกัดหรือสงวนสิทธิ์ไว้โดยเจ้าของซอฟต์แวร์หรือผู้จัดทำ ผู้อื่นไม่สามารถนำมาใช้งาน ทำซ้ำ ดัดแปลง หรือ เผยแพร่ ได้นอกจากได้รับอนุญาตในสิทธิ์นั้นจากเจ้าของ. ซอฟต์แวร์จำกัดสิทธิ์

ผู้ถือกรรมสิทธิ์ซอฟต์แวร์จะไม่ให้ผู้ใช้แก้ไขซอฟต์แวร์ เช่น การปกปิดรหัสต้นฉบับ (Closed source code Software)ของซอฟต์แวร์ได้ หรือ ผู้ถือกรรมสิทธิ์ใช้วิธีทางกฎหมาย เพื่อขัดขวางไม่ให้ผู้ใช้แจกจ่ายซอฟต์แวร์ทั้งที่เป็นของเดิมหรือที่ถูกปรับแต่งโดย ผู้ใช้   
2. สัญญาอนุญาตซอฟต์แวร์แบบเปิด (Open-source License) มีหลายประเภท โดยทั่วไปจะมีข้อกำหนดที่อนุญาตให้ผู้ใช้สามารถดัดแปลงและแจกจ่ายซอฟต์แวร์ต่อได้

ประเภทย่อยของสัญญาอนุญาตซอฟต์แวร์แบบเปิดที่นิยม

* MIT License: อนุญาตให้ผู้ใช้สามารถดัดแปลงและแจกจ่ายซอฟต์แวร์ต่อได้ แต่ต้องระบุว่าซอฟต์แวร์เดิมถูกสร้างโดยผู้เขียนเดิม อนุญาตให้นำซอฟต์แวร์ไปใช้ แก้ไข และแจกจ่ายได้โดยเสรี
* Apache License: อนุญาตให้ผู้ใช้สามารถดัดแปลงและแจกจ่ายซอฟต์แวร์ต่อได้ แต่ต้องระบุว่าซอฟต์แวร์เดิม ถูกสร้างโดยผู้เขียนเดิม และต้องระบุว่าได้มีการดัดแปลง เป็นสัญญาอนุญาตที่ยินยอมสูงและอนุญาตให้ผู้ใช้มีอิสระในการแก้ไขและแจกจ่ายซอฟต์แวร์
* GNU General Public License (GPL): อนุญาตให้ผู้ใช้สามารถดัดแปลงและแจกจ่ายซอฟต์แวร์ต่อได้ แต่ซอฟต์แวร์ที่ดัดแปลงจากซอฟต์แวร์เดิมต้องเป็น open source ด้วย
* Creative Commons Licenses: เป็นสัญญาอนุญาตแบบเปิด ที่ช่วยให้การกระจายซอฟต์แวร์ที่มิฉะนั้นจะ ถูกลิขสิทธิ์ นิยมใช้กับงานสร้างสรรค์

**ชนิดของสัญญาอนุญาตใช้ซอฟต์แวร์**  
• โอเพ่นซอร์ส (Open Source) เป็นซอฟต์แวร์ที่สามารถนำไปใช้งาน ศึกษา แก้ไข และเผยแพร่ได้อย่างเสรีโดยปราศจากเงื่อนไข สามารถนำไปพัฒนาต่อยอด

**แนวคิดหรือปรัชญาที่เกี่ยวกับการใช้และแจกจ่ายซอฟต์แวร์อย่างเสรี**  
**ซอฟต์แวร์เสรี (Free Software**)

มูลนิธิซอฟต์แวร์เสรี (Free Software Foundation : FSF) เป็นองค์กรไม่แสวงหากำไรที่ก่อตั้งโดย ริชาร์ดสตอลล์แมน จดทะเบียนในรัฐแมสซาชูเซตส์ สหรัฐอเมริกา เมื่อวันที่ 4 ตุลาคม พ.ศ. 2528 (ค.ศ. 1985)

เพื่อสนับสนุนแนวทางซอฟต์แวร์เสรี เพื่อต้องการให้สามารถเผยแพร่และแก้ไขซอฟต์แวร์คอมพิวเตอร์ได้โดยปราศจากข้อจำกัดใดๆ

ซอฟต์แวร์เสรีเป็นซอฟต์แวร์ที่ให้ผู้ใช้มีเสรีภาพในการทำสิ่งต่อไปนี้

1. เสรีภาพในการใช้งาน: ผู้ใช้สามารถใช้ซอฟต์แวร์เพื่อวัตถุประสงค์ใดก็ได้
2. เสรีภาพในการศึกษา: ผู้ใช้สามารถศึกษาและแก้ไขซอฟต์แวร์ได้ โดยเข้าถึงซอร์สโค้ด
3. เสรีภาพในการแจกจ่าย: ผู้ใช้สามารถแจกจ่ายสำเนาของซอฟต์แวร์ให้ผู้อื่นได้
4. เสรีภาพในการพัฒนา: ผู้ใช้สามารถปรับปรุงซอฟต์แวร์และเผยแพร่การปรับปรุงเหล่านั้นให้กับผู้อื่นได้

**แนวคิดหรือปรัชญาที่เกี่ยวกับการใช้และแจกจ่ายซอฟต์แวร์อย่างเสรี**  
สัญญาอนุญาตซอฟต์แวร์ที่รองรับแนวคิดซอฟต์แวร์เสรี ได้แก่:

* GNU General Public License (GPL): สัญญาอนุญาตที่ได้รับความนิยมมากที่สุดในหมวดซอฟต์แวร์เสรี ให้เสรีภาพครบทั้ง 4 ข้
* MIT License: สัญญาอนุญาตที่มีข้อกำหนดเรียบง่าย อนุญาตให้ใช้ซอฟต์แวร์ได้โดยไม่มีข้อจำกัดมากนัก
* Apache License: สัญญาอนุญาตที่ให้เสรีภาพในการใช้และแจกจ่ายซอฟต์แวร์ รวมถึงการแก้ไขและแจกจ่ายเวอร์ชันที่แก้ไข

**ซอฟต์แวร์เสรี V.S. ซอฟต์แวร์โอเพนซอร์ส**

* ความเหมือน: ทั้งซอฟต์แวร์เสรีและซอฟต์แวร์โอเพนซอร์สเปิดให้ผู้ใช้สามารถเข้าถึงซอร์สโค้ด ทำการดัดแปลง และแจกจ่ายซอฟต์แวร์ได้ ภายใต้สัญญาอนุญาตที่กำหนด
* ความต่าง:

**ปรัชญา:** ซอฟต์แวร์เสรีเน้นเสรีภาพของผู้ใช้และสิทธิในการควบคุมซอฟต์แวร์ ในขณะที่ซอฟต์แวร์โอเพนซอร์สเน้นประโยชน์ของการพัฒนาซอฟต์แวร์อย่างเปิดเผยและการทำงานร่วมกัน

**มุมมองการใช้งาน:** ซอฟต์แวร์เสรีมุ่งเน้นด้านสังคมและศีลธรรมในการใช้งานซอฟต์แวร์ ส่วนโอเพนซอร์สเน้น ด้านประสิทธิภาพและคุณภาพของซอฟต์แวร์

* ตัวอย่างซอฟต์แวร์ที่เป็นทั้งซอฟต์แวร์เสรีและโอเพนซอร์ส

**GNU/Linux:** ระบบปฏิบัติการที่พัฒนาโดยชุมชน และสอดคล้องกับทั้งแนวคิดซอฟต์แวร์เสรีและโอเพนซอร์ส

**Mozilla Firefox:** เบราว์เซอร์ที่เปิดเผยซอร์สโค้ดและให้สิทธิ์ในการใช้งานและพัฒนาต่อมีเมนูบริบท

**Copyright** มุ่งเน้นการปกป้อง สิทธิ ์ ของผู้สร้างสรรค์ผลงานและให้ สิทธิ ์ เฉพาะแก่ผู้ถือสิทธิ ์ ในการควบคุม การใช้งานผลงาน

**Copyleft** มุ่งเน้นการรักษา เสรีภาพในการใช้งานและแจกจ่าย ผลงาน โดยกําหนดให้ผู้ที่แจกจ่าย ผลงานต้องรักษาเงื่อนไขเสรีภาพเดิมไว

**บทที่ 4 ธุรกรรมอิเล็กทรอนิกส์**

ความสำคัญของกฎหมายธุรกรรมอิเล็กทรอนิกส์

1. สนับสนุนการทำธุรกรรมออนไลน์: เมื่อโลกก้าวเข้าสู่ยุคดิจิทัล การซื้อขายและการทำธุรกรรมต่าง ๆ ส่วนใหญ่ดำเนินการผ่านระบบออนไลน์ กฎหมายธุรกรรมอิเล็กทรอนิกส์ช่วยรับรองความถูกต้องและน่าเชื่อถือของ ธุรกรรมเหล่านี้ เช่น การยอมรับลายเซ็นอิเล็กทรอนิกส์และเอกสารในรูปแบบดิจิทัล ทำให้ธุรกรรมมีผลทางกฎหมายเทียบเท่ากับการใช้เอกสารกระดาษแบบดั้งเดิม
2. เพิ่มความปลอดภัยและป้องกันการปลอมแปลง: ธุรกรรมทางอิเล็กทรอนิกส์ต้องมีมาตรการป้องกันการละเมิดความปลอดภัย เช่น การปลอมแปลงข้อมูล การขโมยข้อมูลส่วนบุคคล กฎหมายธุรกรรมอิเล็กทรอนิกส์กำหนดหลักการและข้อกำหนดทางเทคนิคเพื่อปกป้องความปลอดภัยของธุรกรรม และส่งเสริมให้มีการใช้งานระบบที่ปลอดภัย ﻿﻿﻿
3. สร้างความน่าเชื่อถือ: กฎหมายธุรกรรมอิเล็กทรอนิกส์ช่วยสร้างความเชื่อมั่นให้กับผู้ใช้ในระบบออนไลน์ เช่นการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ที่ได้รับการรับรองจากหน่วยงานที่เชื้อถือได้ ทำให้คู่สัญญา มั่นใจว่าการทำธุรกรรมนั้นถูกต้องตามกฎหมาย
4. รองรับการเติบโตของเศรษฐกิจดิจิทัล: เศรษฐกิจดิจิทัลมีการเติบโตอย่างรวดเร็วและธุรกรรมอิเล็กทรอนิกส์เป็นส่วนสำคัญในการขับเคลื่อนเศรษฐกิจ กฎหมายที่ชัดเจนและทันสมัยช่วยให้การทำธุรกิจและการซื้อขายออนไลน์เป็นไปอย่างราบรื่นและเป็นธรรม
5. จัดการข้อพิพาทและคุ้มครองสิทธิของผู้ใช้: กฎหมายธุรกรรมอิเล็กทรอนิกส์ช่วยให้เกิดความชัดเจนในเรื่อง สิทธิและหน้าที่ของคู่สัญญา เช่น เมื่อเกิดปัญหาข้อพิพาท การเรียกร้องสิทธิหรือคุ้มครองผู้บริโภคสามารถทำได้ภายใต้กรอบกฎหมายที่กำหนด

**ธุรกรรมทางอิเล็กทรอนิกส์ กับ การพาณิชย์เล็กทรอนิกส์ (E-commerce)**

* ธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transaction) หมายถึง กิจกรรมใด ๆ ที่กระทำขึ้นระหว่างหน่วย ธุรกิจ บุคคล รัฐ ตลอดจนองค์กรเอกชนหรือองค์กรของรัฐใด ๆ เพื่อวัตถุประสงค์ทางธุรกิจ การค้า และการ ติดต่องานราชการ โดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน ยกตัวอย่าง เช่น การซื้อ-ขายสินค้า ผ่านเครือข่ายอินเทอร์เน็ต, การพาณิชย์อิเล็กทรอนิกส์, การสมัครสมาชิกผ่านระบบออนไลน์, การตกลงทำ สัญญาซื้อ-ขาย หรือสัญญาตกลงตามข้อบังคับต่างๆ บนเครือข่าย, การโอนเงินด้วยระบบอัตโนมัติผ่านระบบเครือข่าย, การสื่อสารรับ-ส่งข้อมูลอิเล็กทรอนิกส์ด้วยเครือข่ายการสื่อสาร และการสอบถามข้อมูลผ่านระบบออนไลน์ เป็นต้น
* การพาณิชย์เล็กทรอนิกส์ (E-commerce) เป็นการดำเนินกิจกรรมต่าง ๆ ระหว่างผู้ซื้อและผู้ขายที่ครอบคลุมการซื้อการขายสินค้าและบริการ โดยกระทำผ่านสื่ออิเล็กทรอนิกส์ เช่น โทรศัพท์ โทรทัศน์ คอมพิวเตอร์เครือข่ายอินเทอร์เน็ต เป็นต้น เห็นได้ว่า ธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transaction) มีขอบเขตที่กว้างกว่าพาณิชย์อิเล็กทรอนิกส์ (e-commerce)

**พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย**

1. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เป็นกฎหมายหลักที่กำหนดกรอบการทำ ธุรกรรมทางอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อให้ธุรกรรมที่เกิดขึ้นในรูปแบบดิจิทัลมีผลทางกฎหมายเทียบเท่ากับเอกสารกระดาษ
2. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 เป็นการแก้ไขเพิ่มเติมเพื่อปรับปรุงและรองรับการเปลี่ยนแปลงของเทคโนโลยี รวมถึงการกำหนดมาตรฐานสำหรับลายมือชื่อ อิเล็กทรอนิกส์และการทำธุรกรรมภาครัฐ
3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562 ฉบับล่าสุดที่แก้ไขและปรับปรุงเนื้อหาให้ทันสมัย โดยเน้นการปรับปรุงระบบการรับรองลายเซ็นอิเล็กทรอนิกส์และการใช้เทคโนโลยีใหม่ๆเพื่อรองรับการทำธุรกรรมที่ซับซ้อนมากขึ้น

**หลักการสำคัญของกฎหมายธุรกรรมทางอิเล็กทรอนิกส์**

* หลักความเท่าเทียมกัน (Functional Equivalence): ข้อมูลอิเล็กทรอนิกส์จะมีผลทางกฎหมายเทียบเท่า กับเอกสารที่เป็นกระดาษ
* หลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality): กฎหมายไม่จำกัดเฉพาะเทคโนโลยีไดเทคโนโลยีหนึ่ง แต่เปิดโอกาสให้สามารถปรับใช้กับเทคโนโลยีใหม่ๆ ที่เกิดขึ้นในอนาคต
* หลักเสรีภาพในการแสดงเจตนา (Party Autonomy): คู่สัญญามีสิทธิในการกำหนดเงื่อนไขและวิธีการทำ  
  ธุรกรรมของตนเอง

**โครงสร้างของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และฉบับแก้ไขเพิ่มเติม**

* หมวดที่ 1 ธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 7)  
  หมวดนี้กำหนดหลักการที่ให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีผลทางกฎหมายเหมือนกับธุรกรรมแบบ ดั้งเดิม (ที่ใช้เอกสารกระดาษ) หากมีการสร้าง จัดเก็บ หรือส่งข้อมูลในรูปแบบอิเล็กทรอนิกส์ ธุรกรรมนั้นจะมีผลตามกฎหมายเช่นเดียวกับการทำธุรกรรมผ่านเอกสารกระดาษ
* หมวดที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ (มาตรา 26-31)  
  ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) และหลักการที่ให้ลายมือชื่ออิเล็กทรอนิกส์มีผลทางกฎหมายเทียบเท่ากับลายมือชื่อแบบดั้งเดิม โดยลายมือชื่ออิเล็กทรอนิกส์ต้องมีคุณสมบัติตามที่กฎหมายกำหนด เช่น สามารถยืนยัน ตัวตนของผู้ลงนามได้ และมีการป้องกันการปลอมแปลง ซึ่งอาจใช้ ระบบรับรองลายมือชื่อ (Digital Certificate) เพื่อเพิ่มความน่าเชื่อถือ

**ประเภทของลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)**

* ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) คือ ข้อมูลอิเล็กทรอนิกส์ที่ถูกนำมาใช้แทนลายมือชื่อจริงของบุคคล เพื่อแสดงถึงความยินยอม การรับรอง หรือการ ยืนยันตัวตนของบุคคลในธุรกรรมหรือเอกสารทางอิเล็กทรอนิกส์ โดยมีผลทางกฎหมายเช่นเดียวกับลายมือชื่อบนกระดาษ
* ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป (Simple Electronic Signature)  
  ﻿﻿เป็นลายมือชื่อที่ถูกสร้างขึ้นแบบง่าย ๆ เช่น การพิมพ์ชื่อในอีเมล การวาดลายเซ็นด้วยนิ้วหรือปากกาอิเล็กทรอนิกส์ การใช้ภาพลายเซ็นที่สแกนจากเอกสารจริง การกดปุ่ม "ยอมรับ" ในฟอร์มออนไลน์ความปลอดภัยและการยืนยันตัวตนมักไม่สูงมาก และไม่มีการรับรองจากบุคคลที่สาม   
  สะดวกและรวดเร็ว: ผู้ใช้สามารถลงนามได้จากทุกที่และทุกเวลา โดยไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติม  
  ﻿﻿ประหยัดค่าใช้จ่าย: ลดค่าใช้จ่ายในการพิมพ์และส่งเอกสารทางไปรษณีย์  
  ﻿﻿ข้อเสีย  
  ﻿﻿ความปลอดภัยต่ำ: SES อาจถูกปลอมแปลงได้ง่าย เนื่องจากไม่มีการตรวจสอบตัวตนที่เข้มงวด  
  ﻿﻿การรับรองทางกฎหมาย: แม้ว่า SES จะถือว่ามีผลทางกฎหมายในหลายประเทศ แต่ในบางกรณีอาจไม่เพียงพอสำหรับเอกสารที่ต้องการความถูกต้องสูง  
  ﻿﻿การรับรองทางกฎหมาย  
  ﻿﻿ตามกฎหมายหลายประเทศ เช่น กฎหมาย ESIGN ในสหรัฐอเมริกา และระเบียบ eIDAS ในสหภาพยุโรป ระบุว่า SES สามารถถือว่ามีผลทางกฎหมายได้ แต่ระดับความเชื่อถือได้จะต่ำกว่าลายมือชื่ออิเล็กทรอนิกส์ประเภทอื่น ๆ ที่มีการตรวจสอบตัวตนอย่างเข้มงวดมากกว่า
* ลายมือชื่ออิเล็กทรอนิกส์แบบก้าวหน้า (Advanced Electronic Signature)  
  มีการใช้เทคโนโลยีที่ซับซ้อนมากขึ้น เช่น การใช้รหัสผ่าน หรือการยืนยันตัวตนด้วยปัจจัยที่สอง (Two-Factor Authentication) สามารถตรวจสอบและรับรองตัวตนของผู้ลงนามได้ โดยมีคุณสมบัติดังนี้  
  ﻿﻿﻿การเชื่อมโยงกับผู้ลงนาม ลายมือชื่อจะต้องเชื่อมโยงกับผู้ลงนามในลักษณะที่ไม่สามารถโอนถ่ายได้ ซึ่งหมายความว่าผู้ลงนามจะต้องสามารถระบุได้อย่างชัดเจนว่าเป็นผู้ที่ลงนามในเอกสารนั้น  
  ﻿﻿﻿การระบุผู้ลงนาม ต้องสามารถระบุได้ว่าผู้ลงนามคือใคร โดยใช้วิธีการตรวจสอบตัวตนที่เข้มงวด เช่น การใช้รหัส OTP (One-Time Password) หรือการตรวจสอบด้วยข้อมูลประจำตัวอื่น ๆ  
  ﻿﻿﻿การสร้างจากข้อมูลที่ควบคุมได้ ลายมือชื่อจะต้องถูกสร้างขึ้นโดยใช้ข้อมูลการสร้างลายมือชื่อที่ผู้ลงนามสามารถควบคุมได้อย่างเต็มที่ เช่น คีย์ส่วนตัว (private key)  
  ﻿﻿﻿การตรวจสอบความสมบูรณ์ของข้อมูล ลายมือชื่อจะต้องเชื่อมโยงกับข้อมูลที่ถูกลงนามในลักษณะที่สามารถตรวจสอบได้ว่าข้อมูลนั้นไม่ได้ถูกเปลี่ยนแปลงหลังจากที่ได้มีการลงนามแล้ว หากมีการเปลี่ยนแปลงใด ๆ จะทำให้ลายมือชื่อนั้นไม่ถูกต้อง
* ลายมือชื่อดิจิทัล (Digital Signature)

เป็นลายมือชื่อที่ใช้ เทคโนโลยีการเข้ารหัส (Cryptography) และมีการรับรองโดยผู้ให้บริการรับรอง โดยเป็นองค์กรกลางที่มีความน่าเชื่อถือ ซึ่งทำหน้าที่เป็นบุคคลที่สาม เรียกว่า องค์กรออกใบรับรองอิเล็กทรอนิกส์  
(Certification Authority - CA) /เทคโนโลยีการเข้ารหัสแบบ Public Key Infrastructure (PKI)

มีความน่าเชื่อถือและความปลอดภัยสูง เนื่องจากสามารถตรวจสอบตัวตนของผู้ลงนามได้อย่างแน่นอ

นิยมใช้ในธุรกรรมทางการเงินและเอกสารทางกฎหมาย

* หมวดที่ 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 32-34)

กำหนดกฎเกณฑ์เกี่ยวกับ ธุรกิจบริการที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ เช่น ผู้ให้บริการรับรองลายมือชื่ออิเล็กทรอนิกส์ (Certification Authority - CA) กำหนดหน้าที่และความรับผิดชอบของผู้ให้บริการเหล่านี้ในการรับรองและดูแลความปลอดภัยของลายมือชื่ออิเล็กทรอนิกส์

* หมวดที่ 4 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (มาตรา 35)  
  มุ่งเน้นไปที่การใช้เทคโนโลยีในการทำธุรกรรมของภาครัฐ เช่น การให้บริการประชาชนผ่านระบบออนไลน์ ซึ่ง ช่วยเพิ่มความสะดวกในการเข้าถึงบริการของรัฐและส่งเสริมการทำงานของหน่วยงานรัฐให้มีประสิทธิภาพมากขึ้น
* บทบัญญัติมาตรา 35 แห่ง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ว่าด้วยการทำ ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ได้กำหนดให้การทำ "คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูล อิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด" ทั้งนี้ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกียวข้องต้องกระทำหรืองดเว้นการกระทำใดๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้
* หมวดที่ 5 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
* กำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นคณะหนึ่ง เพื่อทำหน้าที่กำกับดูแลและส่งเสริมการทำ ธุรกรรมทางอิเล็กทรอนิกส์ในประเทศไทย โดยมี
* องค์ประกอบของคณะกรรมการ  
  ﻿﻿ประธานกรรมการซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ทรงคุณวุฒิ  
  ﻿﻿ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นรองประธานกรรมการ  
  ﻿﻿กรรมการผู้ทรงคุณวุฒิอื่นซึ่งคณะรัฐมนตรีแ่งตั้งจำนวน 8 คน จากภาครัฐและเอกชน ที่มีความเชี่ยวชาญด้านการเงิน, อีคอมเมิร์ซ, นิติศาสตร์, วิทยาการคอมพิวเตอร์, วิศวกรรมศาสตร์, สังคมศาสตร์ หรือด้านอื่นที่เป็นประโยชน์  
  ﻿﻿ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) เป็นกรรมการและเลขานุการ
* หน้าที่ของคณะกรรมการ  
  ﻿﻿กำหนดนโยบาย แผนงาน และมาตรการในการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์  
  ﻿﻿ออกประกาศ ระเบียบ หรือข้อบังคับเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์  
  ﻿﻿ให้คำปรึกษาและข้อเสนอแนะแก่หน่วยงานของรัฐและเอกชนในการดำเนินการตามกฎหมาย  
  ﻿﻿ปฏิบัติการอื่นใดตามที่กฎหมายกำหนด
* หมวดที่ 6 บทกำหนดโทษ

บทกำหนดโทษ ใน พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (รวมทั้งการแก้ไขเพิ่มเติมในฉบับที่ 2 พ.ศ. 2551 และฉบับที่ 3 พ.ศ. 2562) กำหนดบทลงโทษสำหรับการกระทำที่ฝ่าฝืนกฎหมายเกี่ยวกับ ธุรกรรมทางอิเล็กทรอนิกส์ โดยเน้นเรื่องการปลอมแปลงเอกสารอิเล็กทรอนิกส์ การละเมิดลายมือชื่อ อิเล็กทรอนิกส์ และการปฏิบัติที่ไม่ถูกต้องตามมาตรฐานที่กำหนดไว้

**รายละเอียดของบทกำหนดโทษ**:

1. มาตรา 44

* กำหนดโทษสำหรับผู้ที่ ปลอมแปลงหรือแก้ไขข้อมูลอิเล็กทรอนิกส์ ที่อาจสร้างความเสียหายให้แก่ผู้อื่นหรือทำให้ข้อมูลอิเล็กทรอนิกส์มีความผิดพลาดหรือไม่ถูกต้อง
* โทษ: มีโทษ จำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ หมวดที่ 6 บทกำหนดโทษ

1. มาตรา 45

* กำหนดโทษสำหรับผู้ที่ ใช้หรือเผยแพร่ข้อมูลอิเล็กทรอนิกส์ที่ถูกปลอมแปลงหรือแก้ไข โดยรู้ว่าข้อมูลนั้นถูกปลอมแปลงหรือแก้ไข ซึ่งอาจส่งผลเสียหายต่อบุคคลอื่น
* โทษ: มีโทษ จำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

1. มาตรา 46

* กำหนดโทษสำหรับผู้ที่ ปฏิบัติหน้าที่เป็นผู้ให้บริการรับรอง (Certification Authority - CA) หรือบุคคลอื่น ๆ ที่เกี่ยวข้องกับการให้บริการลายมือชื่ออิเล็กทรอนิกส์ และมีการละเมิดมาตรฐานหรือหลักการที่กำหนดไว้ เช่น การออกใบรับรองโดยไม่ปฏิบัติตามกฎหมาย หรือการจัดการข้อมูลอิเล็กทรอนิกส์อย่างไม่ปลอดภัย
* โทษ: หากการละเมิดกฎดังกล่าวเป็นการกระทำที่เป็นการจงใจหรือมีเจตนาที่ไม่สุจริต มีโทษตามที่กฎหมายกำหนด เว้นแต่จะพิสูจน์ได้ว่าตนมิได้รู้เห็นหรือยินยอมในการกระทำความผิดของนิติบุคคลนั้น

**โครงสร้างของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม**

* พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551  
  มีการเพิ่มเติมและปรับปรุงข้อกำหนดในหลายหมวด เพื่อรองรับการใช้งานลายมือชื่ออิเล็กทรอนิกส์และการทำธุรกรรมที่เกี่ยวข้อง  
  โดยเน้นที่
* เพิ่มบทบัญญัติที่เกี่ยวข้องกับความปลอดภัยในการใช้งานลายเซ็นอิเล็กทรอนิกส์และเอกสารอิเล็กทรอนิกส์
* ปรับปรุงมาตรการในการรับรองลายเซ็นอิเล็กทรอนิกส์ เพื่อให้มีความน่าเชื่อถือและเป็นไปตามมาตรฐานสากล
* พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562

มีการแก้ไขเพิ่มเติมเพื่อรองรับระบบการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์และการพัฒนาธุรกรรมในยุคดิจิทัล เช่นะปรับปรุงเรื่องลายเซ็นอิเล็กทรอนิกส์และการรับรอง โดยเพิ่มมาตรการด้านความปลอดภัยและการยืนยันตัวตนที่มีประสิทธิภาพมากขึ้น เช่น

* การใช้ระบบ PKI (Public Key Infrastructure) และระบบการรับรองดิจิทัล (Digital Certificate) ที่น่าเชื่อถือมากขึ้น
* แก้ไข บทบัญญัติเกี่ยวกับผู้ให้บริการระบบและข้อมูล เพื่อเพิ่มความรับผิดชอบของผู้ให้บริการเกี่ยวกับการจัดการข้อมูลและการทำ ธุรกรรมทางอิเล็กทรอนิกส์อย่างปลอดภัย
* เพิ่มการคุ้มครองผู้บริโภคที่ทำธุรกรรมทางอิเล็กทรอนิกส์มีเมนูบริบท

**บทที่ 5 ความปลอดภัยและอาชญากรรมคอมพิวเตอร์**

**“อาชญากรทางคอมพิวเตอร”** คือ ผูกระทําผิดกฎหมายโดยใชเทคโนโลยี คอมพิวเตอรเปนเครื่องมือสําคัญในการกออาชญากรรมและกระทําความผิด นั้น **“อาชญากรรมทางคอมพิวเตอร”** คือ •การกระทําการใด ๆ เกี่ยวกับการใชคอมพิวเตอร อันทําใหเหยื่อไดรับความเสียหาย และผูกระทําไดรับผลประโยชนตอบแทน •การกระทําผิดกฎหมายใด ๆ ซึ่งใชเทคโนโลยี คอมพิวเตอรเปนเครื่องมือและในการ สืบสวนสอบสวนของเจาหนาที่เพื่อนําผูกระทําผิดมาดําเนินคดีตองใชความรูทาง เทคโนโลยีเชนเดียวกัน

**ลักษณะของอาชญากรรมทางคอมพิวเตอร์**

1. คอมพิวเตอรในฐานะที่เปนวัตถุแหงการกระทําความผิด (Computers as the target of the crime)

ในลักษณะนี้ คอมพิวเตอรเองจะเปนเปาหมายหลักของการโจมตีหรือการกระทํา ความผิด ซึ่งมักจะเกี่ยวของกับการเขาถึงหรือแกไขขอมูลที่อยูในคอมพิวเตอรโดย ไมไดรับอนุญาตตอคอมพิวเตอร (ข้อมูล ระบบ เครือขาย) ไดแก

* การเขาถึงขอมูลหรือระบบคอมพิวเตอรโดยปราศจากอํานาจหน้าที่
* การดักขอมูลคอมพิวเตอร
* การจารกรรมขอมูลคอมพิวเตอร
* การทําใหเกิดความเสียหายตอ ขอมูล ระบบ และเครือขายคอมพิวเตอร

**ตัวอยาง**

* การแฮกเขาระบบคอมพิวเตอร (Hacking) เพื่อเขาถึงข้อมูลหรือระบบโดยไมไดรับ อนุญาต
* การโจมตีดวยมัลแวร เชน ไวรัส โทรจัน หรือแรนซัมแวร เพื่อทําลายหรือขโมยขอมูล
* การทําลายขอมูลในระบบ (Data Destruction) หรือ
* การเปลี่ยนแปลงขอมูลโดยไม ชอบดวยกฎหมาย
* การโจมตีแบบ Distributed Denial of Service (DDoS) เพื่อทําใหระบบ คอมพิวเตอรหรือเว็บไซตไมสามารถใหบริการได

1. คอมพิวเตอรในฐานะที่เปนเครื่องมือที่ใชในการกระทําความผิด (Computers as a tool in the commission of a crime)

ในลักษณะนี้ คอมพิวเตอรจะถูกใชเปนเครื่องมือในการกระทําความผิดทาง อาญา โดยที่คอมพิวเตอรไมใชเปาหมายหลัก แตเปนเครื่องมือที่อาชญากรใช เพื่อชวยใหการกระทําผิดสําเร็จ ตัวอยางเชน

* การเผยแพรภาพลามกอนาจาร
* การเลนการพนันผิดกฎหมาย
* การละเมิดลิขสิทธิ์
* การฟอกเงิน

**ตัวอยาง**

* การฉอโกงทางการเงิน (Fraud) เชน การใชคอมพิวเตอรทําธุรกรรมทางการเงินโดย ผิดกฎหมาย เชน การโอนเงินปลอมแปลง
* การฟอกเงิน (Money Laundering) โดยใชระบบคอมพิวเตอรหรืออินเทอรเน็ตเปน ตัวกลางในการกระจายเงินหรือทรัพยสินที่ไดมาโดยมิชอบ
* การละเมิดลิขสิทธิ์ (Piracy) เชน การใชคอมพิวเตอรเพื่อคัดลอกหรือแจกจายเนื้อหา ที่มีลิขสิทธิ์อยางผิดกฎหมาย
* การสงขอมูลหลอกลวง (Phishing) โดยใชคอมพิวเตอรเพื่อสงอีเมลหรือขอความที่ เปนเท็จเพื่อหลอกลวงใหเหยื่อเปดเผยขอมูลสําคัญ เชน รหัสผานหรือขอมูลบัตร เครดิต

1. คอมพิวเตอรในฐานะที่มีสวนเกี่ยวของกับการกระทําความผิด (Computers as incidental to crime)

ในลักษณะนี้ คอมพิวเตอรไมใชเปาหมายหลักหรือเครื่องมือในการกระทําผิด แตเปนสวนที่เกี่ยวของกับการกระทําผิด อาจใชในการเก็บขอมูลหลักฐานหรือ การจัดการการดําเนินงานของอาชญากร

**ตัวอยาง**

* การจัดเก็บขอมูลหรือหลักฐานการกระทําความผิด (Storage of illegal information) เชน คอมพิวเตอรถูกใชในการเก็บขอมูลที่ไดจากการกระทําผิด เชน ขอมูลการโจรกรรม การขนสงของผิดกฎหมาย
* การติดตอและสื่อสารของกลุมอาชญากร (Communication between criminals) เชน การใชคอมพิวเตอรเพื่อสื่อสารหรือวางแผนการกระทําความผิด
* การใชคอมพิวเตอรในการดําเนินธุรกิจผิดกฎหมาย (Business operation of illegal activities) เชน การใชเว็บไซตหรือระบบคอมพิวเตอรในการขายสินคาผิด กฎหมาย เชน ยาเสพติดหรือสินคาปลอมแปลง

**รูปแบบของการกออาชญากรรมทางคอมพิวเตอร**

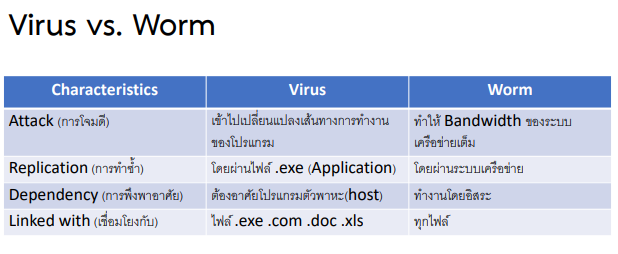
1. การลักลอบเขาถึงโดยไมไดรับอนุญาต ซึ่งกลุมคนที่ลักลอบเข้าถึงขอมูลโดย ไมไดรับอนุญาตสามารถแบงไดเปน 3 กลุมดวยกันคือ

* แฮกเกอร(Hacker) คือกลุมคนที่มีความรูความสามารถและตองการทดสอบ ความสามารถของตนเอง โดยไมมีประสงคราย
* แครกเกอร(Cracker) คือกลุมคนที่มีความรูความสามารถคลายกับ Hackerแต กลุมนี้จะเปนผูที่ประสงคจะทําลายและสรางความเสียหายแกผูอื่น
* สคริปตคิดดี้(Script Kiddy) คือกลุมเด็กหรือนักศึกษาที่เพิ่งจบใหม โดยกลุมนี้จะมี ความตองการอยากทดลอง อยากรูอยากเห็น โดยหลังจะกอกวนผูอื่น

1. การขโมยและทําลายอุปกรณ(Hardware Theft and Vandalism)
2. การขโมยโปรแกรมคอมพิวเตอร(Software Theft)
3. การกอกวนระบบดวยโปรแกรมประสงคราย (Malicious Code)เชน ไวรัส คอมพิวเตอร หนอนอินเตอรเน็ต(WORM) มาโทรจัน(Trojan Horse)
4. การกอกวนระบบดวยสปายแวร(Spyware) สรางความรําคาญ
5. การกอกวนระบบดวยสแปมเมล(Spam Mail) เมลโฆษณา
6. การหลอกลวงเหยื่อเพื่อลวงเอาขอมูลสวนตัว (Phishing)

**อาชญากรคอมพิวเตอร**

ผูกระทําผิดกฎหมายโดยใชเทคโนโลยีคอมพิวเตอรเปนสวนสําคัญ จําแนกไดดังนี้

1. Novice เปนพวกเด็กหัดใหมที่เพิ่งเริ่มหัดใชคอมพิวเตอร หรืออาจหมายถึงพวกที่เพิ่งไดรับความไววางใจ ใหเขาสูระบบเครือขายคอมพิวเตอร
2. Deranged person คือ พวกจิตวิปริต ผิดปกติ มีลักษณะเปนพวกชอบความรุนแรง และอันตรายมัก เปนพวกที่ชอบทําลายทุกสิ่งที่ขวางหนาไมวาจะเปนบุคคล สิ่งของ หรือสภาพแวดลอม
3. Organized Crime กลุมอาชญากรที่รวมมือกันทําผิดในลักษณะขององคกรใหญๆ เหมือนองคกรธุรกิจ ทั่วไป ที่มีระบบ จะใชคอมพิวเตอรที่ตางกัน โดยสวนหนึ่งอาจใชเปนเครื่องหาขาวสาร อีกสวนหนึ่งก็จะใช เทคโนโลยีเพื่อเปนตัวประกอบสําคัญในการกออาชญากรรม หรือใชเทคโนโลยีกลบเกลื่อนรองรอย ใหรอด พนจากเจาหนาท
4. Career Criminal พวกอาชญากรมืออาชีพ เปนกลุมอาชญากรคอมพิวเตอรที่มีอยู มาก กลุมนี้นาอันตรายมากที่สุด
5. Com Artist เปนพวกที่ชอบความกาวหนาทางคอมพิวเตอร เพื่อใหไดมาซึ่ง ผลประโยชนสวนตน อาชญากรประเภทนี้จะใชความกาวหน เกี่ยวกับระบบคอมพิวเตอร และความรูของตนเพื่อหาเงินแบบผิดกฎหมาย
6. Dreamer พวกบาลัทธิ เปนพวกที่คอยทําผิดเนื่องจากมีความเชื่อถือสิ่งหนึ่งสิ่งใดอยาง รุนแรง
7. Cracker เปนผูที่มีความรูและทักษะทางคอมพิวเตอรเปนอยางดี จนสามารถลักลอบ เขาสูระบบได โดยมีวัตถุประสงคเขาไปหาผลประโยชนอยางใดอยางหนึ่ง มักเขาไปทําลาย หรือลบไฟล หรือทําใหคอมพิวเตอรใชการไมได รวมถึงทําลายระบบปฏิบัติการ

**พระราชบัญญัติวาดวยการกระทําความผิดเกี่ยวกับคอมพิวเตอร**

* ฉบับที่ 1 พ.ศ. 2550 เปนกฎหมายพื้นฐานที่ถูกนํามาใชในยุคเริ่มตนของ อาชญากรรมทางไซเบอรในประเทศไทย เนนไปที่การควบคุมการกระทําผิด ทางคอมพิวเตอรในรูปแบบที่ยังไมซับซอนมากนัก
* ฉบับที่ 2 พ.ศ. 2560 ไดรับการปรับปรุงใหทันสมัยกับสถานการณปจจุบัน โดยเพิ่มบทบัญญัติใหมๆ เกี่ยวกับการควบคุมเนื้อหาออนไลน การลงโทษผูให บริการ และการเพิ่มความเขมงวดในบทลงโทษ

การประกาศใช พระราชบัญญัติวาดวยการกระทําความผิดเกี่ยวกับ คอมพิวเตอร (ฉบับที่ 2) พ.ศ. 2560 ไมได **ยกเลิก** พระราชบัญญัติฉบับเดิมที่ ออกใน พ.ศ. 2550 แตเปนการ แกไขเพิ่มเติม ขอกฎหมายในบางสวนของ พระราชบัญญัติ พ.ศ. 2550 เพื่อปรับปรุงใหสอดคลองกับสถานการณในยุค ปจจุบันมากขึ้น

ดังนั้น พระราชบัญญัติ พ.ศ. 2550 ยังคงมีผลบังคับใช แตถูกแกไขและ เพิ่มเติมบางมาตราเพื่อใหเหมาะสมและมีประสิทธิภาพมากขึ้นในการจัดการ กับอาชญากรรมทางคอมพิวเตอรที่เปลี่ยนแปลงไปตามยุคสมัย เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60

**เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60**

1. การควบคุมเนื้อหา (Content Control)

* พ.ศ. 2550: การควบคุมเนื้อหาอยูใน มาตรา 14 ซึ่งระบุถึงการนําเขาสูระบบคอมพิวเตอรดวยขอมูล ที่เปนเท็จ ขอมูลที่เปนภัยตอความมั่นคง หรือขอมูลที่อาจกอใหเกิดความเสียหายแกผูอื่น
* มาตรา 14(1): การนําเขาขอมูลเท็จที่อาจกอใหเกิดความเสียหายแกผูอื่น
* มาตรา 14(2): ขอมูลที่อาจกอใหเกิดความเสียหายตอความมั่นคงของประเทศ
* มาตรา 14(3): ขอมูลที่เปนภัยตอความปลอดภัยของสาธารณะ
* พ.ศ. 2560: การแกไขเพิ่มเติมใน มาตรา 14 ขยายความถึงการควบคุมเนื้อหาออนไลนใหละเอียดขึ้น โดยเนนการควบคุมเนื้อหาที่เกี่ยวกับความมั่นคงของประเทศและความสงบสุขในสังคม มีบทลงโทษที่ หนักขึ้นสําหรับผูเผยแพรขอมูลเท็จที่กระทบตอความมั่นคงและสังคม เชน มาตรา 14(1) ถึง (5) ซึ่ง อางอิงถึงการนําขอมูลที่ไมเปนความจริงเขาสูระบบคอมพิวเตอร หรือขอมูลที่อาจกอใหเกิดความตื่น ตระหนกแกประชาชน เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60

1. การเก็บรักษาขอมูล (Data Retention)

* พ.ศ. 2550: ระบุใน มาตรา 26 ที่กําหนดใหผูใหบริการตองเก็บบันทึกขอมูลการจราจร ทางคอมพิวเตอร (Log File) เปนเวลาไมนอยกวา 90 วัน
* พ.ศ. 2560: มีการแกไขใน มาตรา 26 เพิ่มเติมในสวนของความยืดหยุนใหสามารถ ขยายระยะเวลาการเก็บขอมูลไดมากกวา 90 วันตามความจําเปน เพื่อใชในการสืบสวน คดีและติดตามการกระทําผิดทางไซเบอรไดอยางมีประสิทธิภาพยิ่งขึ้น เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60

1. บทลงโทษสําหรับผูใหบริการ (Service Provider Liability)

* พ.ศ. 2550: กฎหมายฉบับนี้ไมไดระบุชัดเจนเกี่ยวกับบทลงโทษสําหรับผูใหบริการที่ไม สามารถควบคุมเนื้อหาบนแพลตฟอรมได
* พ.ศ. 2560: ใน มาตรา 15 ไดเพิ่มขอกําหนดวาผูใหบริการที่มีหนาที่จัดเก็บขอมูลที่ผิด กฎหมาย หรือไมลบขอมูลตามคําสั่งของเจาหนาที่ จะมีโทษจําคุกไมเกิน 5 ป หรือปรับ ไมเกิน 100,000 บาท หรือทั้งจําทั้งปรับ เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60

1. บทลงโทษสําหรับการนําขอมูลเท็จเขาสูระบบคอมพิวเตอร (False Information)

* พ.ศ. 2550: ระบุใน มาตรา 14 การนําขอมูลเท็จเขาสูระบบคอมพิวเตอรที่อาจ กอใหเกิดความเสียหายแกบุคคลอื่น
* พ.ศ 2560: ใน มาตรา 14(1) ถึง (5) มีการขยายความเรื่องการนําขอมูลเท็จเขาสูระบบ คอมพิวเตอรที่อาจทําใหสังคมเกิดความเขาใจผิด หรือกอใหเกิดความเสียหายตอความ มั่นคงของชาติ โดยมีบทลงโทษที่เพิ่มขึ้น เปรียบเทียบ พ.ร.บ. คอมฯ ป 50 กับ ป 60

1. ความผิดฐานหมิ่นประมาท (Defamation)

* พ.ศ. 2550: ใน มาตรา 14 ยังรวมถึงความผิดฐานหมิ่นประมาท ซึ่งผูกระทําการหมิ่น ประมาทผานระบบคอมพิวเตอรจะถูกลงโทษภายใตพระราชบัญญัตินี้
* พ.ศ. 2560: ใน ฉบับที่ 2 พ.ศ. 2560 ความผิดฐานหมิ่นประมาทไดถูก ยกเลิก ออกจาก พระราชบัญญัตินี้ ผูกระทําการหมิ่นประมาทออนไลนจะถูกดําเนินการตาม ประมวล กฎหมายอาญา มาตรา 326 และ 328 แทน

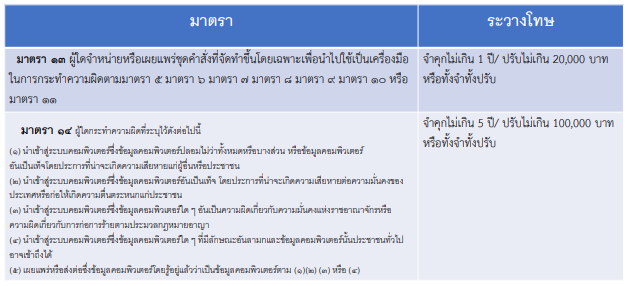
**ลักษณะความผิดใน พรบ**

1. การเขาถึงระบบคอมพิวเตอรโดยไมไดรับอนุญาต

การกระทํานี้จะผิดกฎหมายตั้งแตการพยายามเขาถึงระบบที่ไมไดรับอนุญาต โดยไมมีการทําลายหรือแกไขขอมูล

1. การลวงรูมาตรการปองกัน

เมื่อมีการเขาถึงและลวงรูขอมูลเกี่ยวกับมาตรการปองกัน เชน รหัสผาน หรือ ระบบรักษาความปลอดภัย แลวนําไปเปดเผยใหผูอื่นทราบ จะถือวาผิดกฎหมาย

1. การเขาถึงขอมูลโดยมิชอบ

การเขาถึงขอมูลคอมพิวเตอรของผูอื่นโดยไมไดรับอนุญาต รวมถึงการเจาะ ระบบเพื่อดูขอมูลที่ควรจะเปนสวนตัวของบุคคลอื่น

1. การดักรับขอมูลโดยมิชอบ

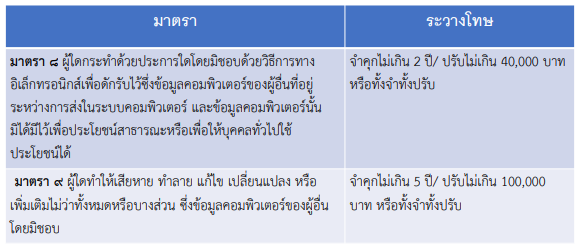
การดักรับขอมูลที่อยูระหวางการสงผานในระบบคอมพิวเตอร โดยไมไดรับ อนุญาตจากเจาของขอมูล เชน การดักฟงอีเมลหรือขอความ

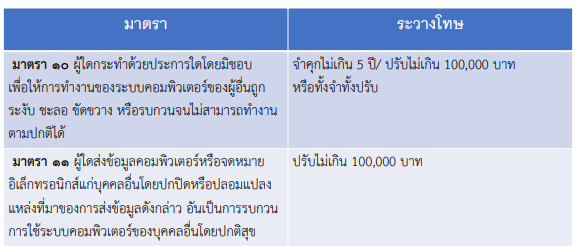
1. การทําใหเสียหาย ทําลาย หรือแกไขขอมูล

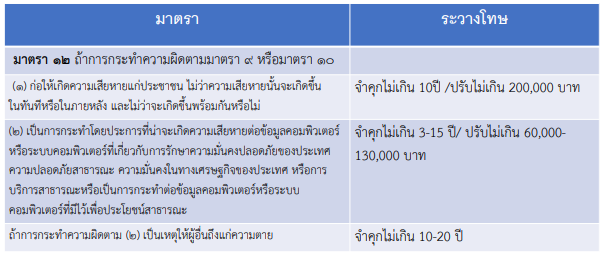
การลบ เปลี่ยนแปลง แกไข หรือทําลายขอมูลของผูอื่นโดยมิชอบ ถือเปนการ ทําความผิดที่รุนแรงยิ่งขึ้น

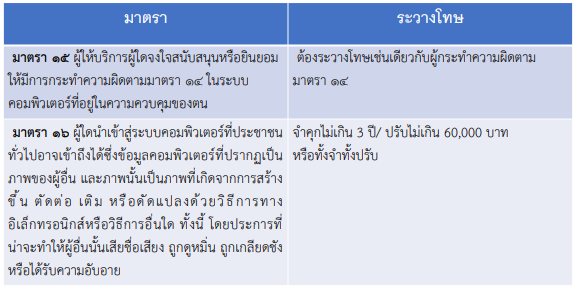
1. การระงับ ชะลอ ขัดขวาง หรือรบกวนระบบ

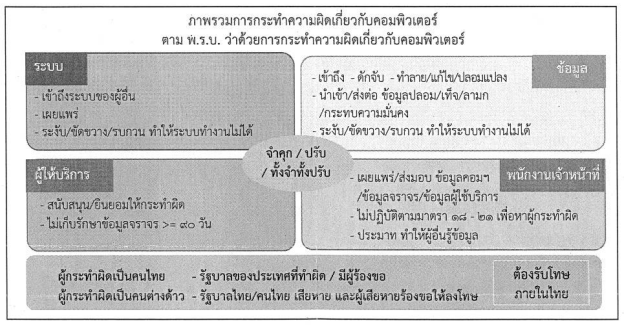
การกระทําที่ขัดขวางการทํางานของระบบคอมพิวเตอร เชน การโจมตีแบบ Distributed Denial of Service (DDoS) ถือเปนการรบกวนระบบที่มีโทษรุนแรง











**บทที่ 6 พรบคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**

* **การคุมครอง** ขอมูลสวนบุคคล แตใจความสําคัญของกฎหมายฉบับนี้ กลับมุงเนนไปที่องคกร หนวยงาน หรือนิติบุคคลใหมี “มาตรฐาน” ในการจัดการขอมูลสวนบุคคลอยางเหมาะสมและ เพียงพอ
* เพื่อปองกันความเสี่ยงที่จะมีผลกระทบไปถึง
* การรักษาความลับ (Confidentiality)
* ความถูกตองสมบูรณ (Integrity)
* และความพรอมใชงาน (Availability)

ของขอมูลสวนบุคคล ที่กอใหเกิดแนวโนมใหเกิดผลกระทบเชิงลบหรือความเสียหายในระดับบุคคล หรือองคกร

พระราชบัญญัติขอมูลสวนบุคคล พ.ศ. 2562 (พ.ร.บ.คุมครองขอมูลสวนบุคคล) หรือ PDPA (Thailand’s Personal Data Protection Act B.E. 2562 (2019))

* ประกาศในราชกิจจานุเบกษาในวันที่ 27 พฤษภาคม 2562
* จะมีผลบังคับใชวันที่ 28 พฤษภาคม 2563

**ขอมูลสวนบุคคล** หมายถึง ขอมูลเกี่ยวกับบุคคลซึ่งทําใหสามารถระบุตัวบุคคลนั้น ได ไมวาทางตรงหรือทางออม เชน ชื่อ ที่อยู เบอรโทรศัพท อีเมล

**ผูควบคุมขอมูล** หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอํานาจหนาที่ตัดสินใจเกี่ยวกับการ เก็บรวบรวม ใช หรือเปดเผยขอมูลสวนบุคล

* ระบบสมาชิกหรือการลงทะเบียน ไมวาจะเปนเว็บไซต Application หรือสื่อดิจิทัลอื่น ๆ ไมวาจะออนไลนหรือออฟไลน ก็ถือวาเปนผูควบคุมขอมูลสวนบุคคลเชนกัน

**ผูประมวลผลขอมูล** หมายถึง บุคคลหรือนิติบุคคลซึ่งดําเนินการเกี่ยวกับการเก็บ รวบรวม ใช หรือเปดเผยขอมูลสวนบุคคลตามคําสั่งหรือในนามของผูควบคุมขอมูล สวนบุคคล แตไมไดเปนผูควบคุมขอมูลเอง

ดังนั้น Agency และผูใหบริการ Hosting Server ที่เก็บขอมูล ถือเปนผูประมวลผล ไมใช ผูควบคุม

**หลักทั่วไปของ พ.ร.บ.**

1. เจาของขอมูลตองใหความยินยอม (Consent) ในการเก็บรวบรวม การใช และการเปดเผย ขอมูลสวนบุคคลตามวัตถุประสงคที่ผูเก็บรวบรวม ผูใช แจงไวตั้งแตแรกแลวเทานั้น (ตองขอ อนุมัติจากเจาของขอมูลกอน) เชน หากแอปพลิชันหนึ่งจะเก็บขอมูลบัตรเครดิตของเราไวใน ระบบ ก็ตองมีขอความใหเรากดยืนยันเพื่อยินยอม พรอมแจงวัตถุประสงคในการเก็บรวบรวม และการใช หากเราไมยินยอมใหใชขอมูลบัตรเครดิต ผูใหบริการแอปพลิเคชันนั้นก็ไมสามารถใช ขอมูลบัตรเครดิตของเราได
2. ผูเก็บรวบรวมขอมูลตองรักษาความมั่นคงปลอดภัยของขอมูล ไมใหมีการเปลี่ยนแปลงแกไข หรือถูกเขาถึงโดยผูที่ไมเกี่ยวของกับขอมูล เชน สถานพยาบาลจะตองเก็บขอมูลของผูปวยให เปนความลับและไมเปดเผยใหกับผูอื่น ธนาคารตองเก็บรักษาขอมูลเกี่ยวกับรายการถอน
3. เจาของขอมูลมีสิทธิ์ถอนความยินยอม ขอใหลบหรือทําลายขอมูลเมื่อใดก็ได หากเปนความ ประสงคของเจาของขอมูล

**บทลงโทษ** หากผูเก็บรวบรวมขอมูลฝาฝน จะมีบทลงโทษทั้งทางอาญา และทางปกครอง โดยมี

* โทษทางอาญาคือ จําคุกไมเกิน 6 เดือนถึง 1 ป หรือปรับไมเกิน 5 แสน – 1 ลานบาท,
* โทษทางปกครอง มีโทษปรับตั้งแตไมเกิน 5 แสนบาท-5 ลานบาท

**ข้อยกเว้น**

มาตรา 4

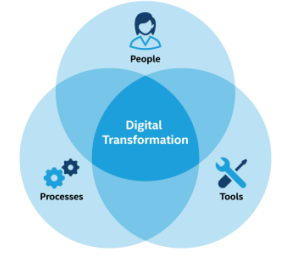
* การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูล และต้องเป็นไปเพื่อประโยชน์ส่วนตน หรือกิจกรรมในครอบครัวของเจ้าของข้อมูลเท่านั้น
* การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ หรือรักษาความปลอดภัยของประชาชน รวมถึงหน่วยงานด้านการป้องกันและปราบปรามการทุจริต หรือทางด้านวิทยาศาสตร์ ที่จำเป็นเพื่อการคุ้มครองประโยชน์สาธารณะ
* บุคคลที่เก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อตอบสนองงานศิลปกรรม วรรณกรรม วิชาการ หรือการรวบรวมสถิติเพื่อประโยชน์ส่วนรวม
* สถาบันพระมหากษัตริย์ รัฐสภา และรัฐธรรมนูญ รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสถาบันดังกล่าว สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ตามหน้าที่และอำนาจของสถาบันพระมหากษัตริย์ รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
* การดำเนินการเกี่ยวกับข้อมูลของจำเลยหรือผู้ต้องหาในคดีอาญาและสถิติทางกฎหมายที่จำเป็นต่อกระบวนการยุติธรรมทางอาญา
* การยกเว้นไม่ต้องขอความยินยอมตามพระราชบัญญัติ สำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลได้เปิดเผยต่อสาธารณะ หรือเป็นไปเพื่อประโยชน์สาธารณะ โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล

**แนวทางการเตรียมตัวของนักพัฒนา/เจาของระบบ**

1. ในเว็บไซต Application หรือสื่อดิจิทัลอื่น ๆ ที่จะตองระบุวัตถุประสงคของการ เก็บ ใช หรือเปดเผยขอมูลสวนตัว ในภาษาที่เขาใจงายและตรงไปตรงมา ‘นโยบายความเปนสวนตัว’ (Privacy Policy)
2. ทุกครั้งที่ใหผูใชงานลงทะเบียนหรือกรอกขอมูลสวนบุคคล ควรมีตัวเลือกแบบ Checkbox ใหผูใชงานกดเลือกเพื่อยืนยันความยินยอมจากเจาของขอมูล และ มี link เพื่อกดเขาดูรายละเอียดหนาวัตถุประสงคของการเก็บ ใช หรือเปดเผย ขอมูลสวนตัวนั้นดวย แนวทางการเตรียมตัวของนักพัฒนา/เจาของระบบ
3. ควรมีชองทางติดตอและมีหนารายละเอียดที่ระบุวา หากผูใชงานตองการที่จะ ติดตอเพื่อขอตรวจสอบหรือขอรับสําเนาขอมูลสวนบุคคลเกี่ยวกับตน ตองติดตอหา แบรนดและธุรกิจอยางไร โดยอาจจะเพิ่มปุม ‘ติดตอเพื่อขอตรวจสอบขอมูลสวนบุคคล’ ใน Footer หรือหนา Contact Us ในเว็บไซตหรือ Application นั้นดวย
4. ควรมีชองทางใหผูใชงานเจาของขอมูลแจงขอยกเลิกความยินยอมที่เคยใหไปและ ลบขอมูลสวนบุคคลที่ตัวเองเปนเจาของออกจากระบบการจัดเก็บของแบรนดและ ธุรกิจได โดยอาจจะเปน link ‘ยกเลิกความยินยอมจัดเก็บและใชงานขอมูลสวนบุคคล’ เพื่อเขาหนาเว็บที่มีรายละเอียดวิธีการแจงความตองการดังกลาว

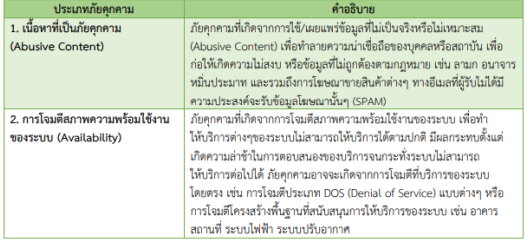
**บทที่ 7 การรักษาความมั่นคงปลอดภัยไซเบอร์**

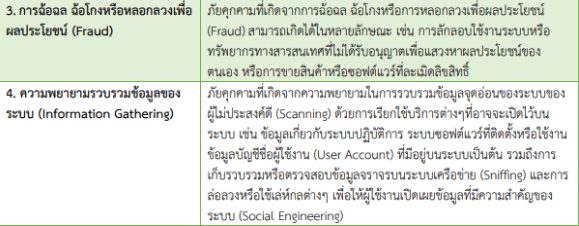
**ปรากฎการณ์ DX (Digital Transformation)**

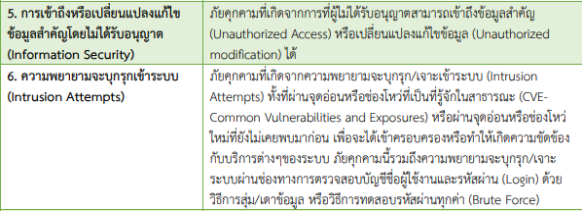
****

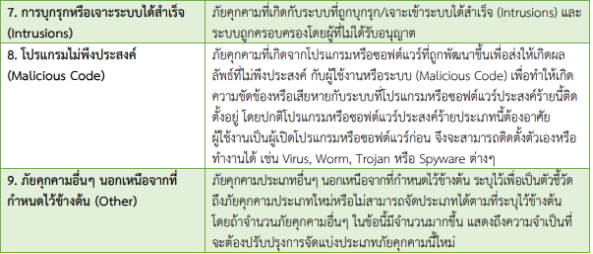
**กฎหมานที่เกิดจา DX**

****

**ประเภทภัยคุมคามทางไซเบอร์ของไทย**

****

****

****

**ความหมายของความมั่นคงปลอดภัยไซเบอร์**

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ

* กระบวนการหรือการกระทําทั้งหมดที่จําเป็นเพื่อทําให้องค์กรปราศจากความเสี่ยง และ ความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการก่ออาชญากรรม การโจมตี การบ่อนทําลาย การจารกรรม และความผิดพลาดต่างๆ
* โดยจะคํานึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล (CIA) 3 ประการคือ

1. การรักษาความลับของข้อมูล (Confidentiality)
2. การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity)
3. ความพร้อมในการใช้งานของข้อมูล (Availability)

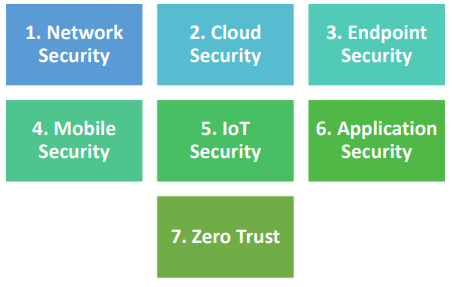
ประเภทภัยคุกคามทางไซเบอร์

**“ไมรายแรง”** หมายถึง ภัยคุกคามที่มีความเสี่ยงทําให ระบบคอมพิวเตอรหรือบริการของรัฐดอpประสิทธิภาพลง

“รายแรง” หมายถึง การโจมตีระบบ มุงเปาที่ ทําใหบริการ ภาครัฐ ความมั่นคงของรัฐ การปองกันประเทศ เศรษฐกิจ สาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบ เรียบร้อยของประชาชนเสียหายจนไมสามารถทํางานหรือใช บริการได

**“วิกฤต”** มีการโจมตีที่สงผลกระทบรุนแรงในวงกวาง ทําใหระบบลมเหลวจนรัฐไม สามารถควบคุมได มีความเสี่ยงที่จะลามไปยังโครงสรางพื้นฐานสําคัญอื่น ๆ หรือ เปนภัยที่กระทบตอความสงบเรียบรอยของประชาชนหรือความมั่นคงของรัฐ หรือ อาจทําใหประเทศหรือสวนใดสวนหนึ่งตกอยูในภาวะคับขัน

**ประเภทของความปลอดภัยทางไซเบอร์**

****

**ความสําคัญของกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์**

* เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย ITของโครงสร้างพื้นฐานที่สําคัญทาง สารสนเทศ หรือ บริการที่สําคัญของประเทศ มีความมั่นคงปลอดภัยสามารถให้บริการได้ เป็นปกติ และหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ ได้อย่างทันท่วงที
* พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ เน้นไปที่หน่วยงานโครงสร้างพื้นฐานที่มี ความสําคัญของประเทศ (Critical Infrastructure) เช่น โรงไฟฟ้า ผู้ให้บริการเครือข่าย โทรคมนาคม รถไฟฟ้าทั้งบนดินและใต้ดิน สนามบินทั้งในเมืองหลวงและหัวเมืองต่างๆ สถาบันการเงิน ธนาคารแห่งประเทศไทย ตลาดหลักทรัพย์ หน่วยงานด้านสาธารณสุข ทั้ง โรงพยาบาลของรัฐและโรงพยาบาลเอกชน หน่วยงานรัฐในการให้บริการประชาชน

(**Critical Information Infrastructure) CII**

คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการ ของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทาง เศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

**ภัยคุกคามทางไซเบอร์**

การกระทําหรือดําเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิด การประทุษร้ายต่อระบบคอมพิวเตอร์ ทรัพย์สินทางสารสนเทศ และเป็น ภัยอันตรายที่ใกล้จะถึงหรือที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบ ต่อการทํางานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือทรัพย์สินทาง สารสนเทศ

**ประโยชน์ของ พรบ ไซเบอร์**

****

**การดําเนินการด้าน Cyber security ในองค์กร**

องค์กรจะต้องดําเนินการ Cyber security ให้ครอบคุลมทั้ง People, Processes & Technology

1. People : พนักงาน/บุคลากร

* พนักงานในองค์กรทุกคนควรจะรับรู้ หรือเข้าใจเกี่ยวกับบทบาทของตัวเองในการป้องกัน และลด Cyber Threats และให้เข้าใจวิธีการดูเมลที่มีความเสี่ยงว่าจะเป็น Malware ชึ่งเป็นปัญหาของภาค ธุรกิจ และทุกคนจะมีบทบาทที่สําคัญ โดยหากเข้าใจโปรแกรมที่ช่วยด้านความปลอดภัยจะทําให้ลด ความเสี่ยงได้
* ผู้เชี่ยวชาญทางด้านความปลอดภัยทาง Cyber ในองค์กรควรที่จะเรียนรู้ทักษะเพิ่มเติมเพื่อให้ แน่ใจว่าสามารถควบคุมเทคโนโลยี และการปฎิบัติที่จะแก้ไข Threats ได้อย่างเหมาะสม

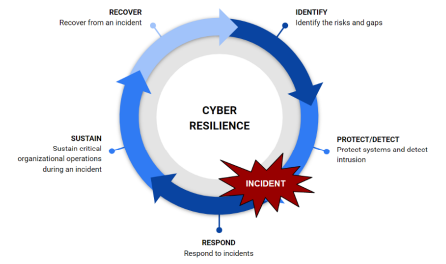
1. Processes : ปรับกระบวนการ ซึ่งส่วนที่สําคัญต่อการปรับปรุงกลยุทธ์ด้าน Cyber Security เพื่อตรวจสอบ กิจกรรม หรือบทบาทในองค์กร ที่จะสามารถลดความเสี่ยง ต่อข้อมูลภายใน เนื่องจากภัยคุกคามทางไซเบอร์เปลี่ยนแปลงไปอย่างรวดเร็ว ดังนั้น กระบวนการจําเป็นต้องปรับตัวให้พร้อมรับมืออยู่ตลอด
2. Technology ต้องมีการวิเคราะห์ระดับความเสี่ยงของภัยคุมคามต่าง ๆ ในองค์กร ได้แก่ ภัยทาง ธรรมชาติ หรือ ภัยทางไซเบอร์ หาปัจจัยที่สามารถลดความเสี่ยงทางไซเบอร์ ที่ขึ้นอยู่กับการ ประเมินความเสี่ยง หรือจะยอมรับความเสี่ยง

**หน่วยงานหลักที่เกี่ยวข้อง**

1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES): ทําหน้าที่กํากับดูแลนโยบายและแนว ทางการดําเนินการในด้านดิจิทัลและความมั่นคงไซเบอร์ https://www.ncsa.or.th/index.html
2. สํานักงานคณะกรรมการการรักษาความมั ่นคงปลอดภัยไซเบอร์แห่ งชาต ิ(NCSA): เป็นหน่วยงานหลักที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
3. ศูนย์ปฏิบัติการความมั ่นคงปลอดภัยไซเบอร์ (CERT): รับผิดชอบในการตรวจสอบและ ตอบสนองต่อภัยคุกคามไซเบอร์
4. หน่วยงานภาครัฐและเอกชน: ที่มีการดําเนินการที่เกี่ยวข้องกับโครงสร้างพื้นฐานสําคัญ ของประเทศ เช่น สถาบันการเงิน สาธารณสุข พลังงาน และการคมนาคม เป็นต้น

**Cyber Resilience**

* ความสามารถในการเตรียมตัว และตอบสนองตอภัยคุกคามทางไซเบอร รวมถึงการกูคืนระบบให กลับมาดําเนินการไดตามปกติ
* มุ่งเน้นไปในเรื่องความพร้อมหรือการปรับตัวเพื่อรับมือกับสถานการณ์ที่เกี่ยวข้องกับภัย คุกคาม
* ซึ่งจะแตกต่างกับ Cyber Security ที่เน้นไปในทางการป้องกันเพื่อไม่ให้เกิด



**หลักการสําคัญของ Cyber Resilience**

1. การระบุความเสี่ยง (Identify): ประเมินความเสี่ยงและวางแผนในการจัดการภัย คุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อองค์กร ในด้าน การบริหารจัดการภายใน องค์กร บุคลากร ความสามารถ ข้อมูลและระบบภายใน ทรัพย์สินทั้งหมดขององค์กร
2. การป้องกัน (Protect): เริ่มตั้งแต่การวางกลไกและขั้นตอนเพื่อรักษาความปลอดภัย การติดตั้งอุปกรณ์ เช่น Firewall การบํารุงรักษาอุปกรณ์ กระบวนการจัดการข้อมูล และ การควบคุมการเข้าถึงและการใช้ระบบ นอกจากนี้ยังรวมถึงการฝึกอบรมและสร้างความ ตระหนักให้บุคลากร หลักการสําคัญของ Cyber Resilience
3. การตรวจจับ (Detect): การเฝ้าระวังและติดตามเหตุการณ์หรือกิจกรรมน่าสงสัยที่ อาจก่อให้เกิดภัยคุกคามทางไซเบอร์ซึ่งมีผลกระทบต่อองค์กร รวมถึงการตรวจสอบหาช่อง โหว่ของระบบ
4. การตอบสนอง (Respond): เมื่อมีการตรวจสอบและพบความผิดปกติที่มีผลต่อความ ปลอดภัย มีการวางแนวทางปฏิบัติให้ชัดเจน มีการวิเคราะห์หาสาเหตุ และมีการสื่อสารกัน ระหว่างองค์กร เพื่อแก้ไขหรือลดปัญหาแบบเดิมขึ้น
5. การกู้คืน (Recover): ทําให้ระบบกลับมาใช้งานได้เป็นปกติอย่างรวดเร็วที่สุด ให้ธุรกิจ ดําเนินต่อไปได้อย่างต่อเนื่อง และลดความสูญเสีย ต้องมีการวางแผนการกู้คืนอย่างมีระบบ

**บทที่ 2 จรราบรรณในวิชาชีพ**

**Ethic code 1**. Product (จรรยาบรรณตอการผลิต/ผลผลิต) **หลักการสําคัญ:**

1. การพัฒนาซอฟตแวรที่มีคุณภาพ:

* การสรางและพัฒนาซอฟตแวรที่มีความเสถียร ปราศจากบั๊ก และสามารถทํางานไดตามที่ออกแบบไว
* การทดสอบและตรวจสอบซอฟตแวรอยางละเอียดเพื่อใหแนใจวามีคุณภาพสูงสุด

1. การรับผิดชอบตอความปลอดภัย:

* การปกปองขอมูลผูใชและขอมูลสําคัญจากการถูกเขาถึงโดยไมไดรับอนุญาต
* การใชมาตรการรักษาความปลอดภัยในการพัฒนาซอฟตแวร เชน การเขารหัสขอมูล การตรวจสอบความถูกตองของขอมูล และการปองกันการโจมตีจากภายนอก

1. การใหประโยชนตอผูใชงาน:

* การพัฒนาซอฟตแวรที่ตอบสนองตอความตองการและความคาดหวังของผูใช
* การออกแบบซอฟตแวรที่ใชงานงายและเปนมิตรกับผูใช (User-friendly)
* การใหบริการหลังการขายและการสนับสนุนที่ดีเพื่อชวยแกไขปญหาของผูใช

1. การปฏิบัติตามมาตรฐานและกฎหมายที่เกี่ยวของ:

* การปฏิบัติตามมาตรฐานการพัฒนาซอฟตแวรที่กําหนดโดยองคกรวิชาชีพและหนวยงานที่เกี่ยวของ เชน IEEE, ISO
* การปฏิบัติตามกฎหมายและระเบียบขอบังคับที่เกี่ยวของกับการพัฒนาซอฟตแวร

1. การคํานึงถึงผลกระทบตอสังคมและสิ่งแวดลอม:

* การพัฒนาซอฟตแวรที่ไมกอใหเกิดผลกระทบทางลบตอสังคมและสิ่งแวดลอม
* การสนับสนุนการใชทรัพยากรอยางมีประสิทธิภาพและการลดการปลอยกาซเรือนกระจก

มุงมั่นในการพัฒนาซอฟตแวรที่มีคุณภาพ ปลอดภัย และ เปนประโยชนตอผูใชงา

**กรณีตัวอยาง**

บริษัท A พัฒนาซอฟตแวรสําหรับการจัดการขอมูลลูกคาของ ธนาคาร ซึ่งจะตองมีความปลอดภัยสูง บริษัทไดใชเวลา ทดสอบซอฟตแวรอยางละเอียดทุกขั้นตอนเพื่อตรวจหา ขอบกพรองและชองโหว เมื่อพบปญหาในกระบวนการ เขารหัสขอมูล ทีมพัฒนาไดทําการแกไขอยางรวดเร็วและ ทดสอบใหมจนมั่นใจวาไมมีปญหาเหลืออยูกอนที่จะปลอย ซอฟตแวรใหกับธนาคาร

**Ethic code 2**. Public (จรรยาบรรณตอบริบท)

**หลักการสําคัญ**:

1. การปกปองความปลอดภัยของสาธารณะ:

* การพัฒนาซอฟตแวรที่ไมกอใหเกิดอันตรายหรือความเสี่ยงตอผูใชงานและสาธารณะ
* การตรวจสอบและประเมินความเสี่ยงของซอฟตแวรตอความปลอดภัยของสาธารณะอยางรอบคอบ

1. การสงเสริมสุขภาพและความเปนอยูที่ดีของสาธารณะ:

* การพัฒนาซอฟตแวรที่สงเสริมสุขภาพและความเปนอยูที่ดีของผูใชและสังคม
* การคํานึงถึงผลกระทบทางสุขภาพที่อาจเกิดขึ้นจากการใชซอฟตแวร

1. การปกปองขอมูลสวนบุคคล:

* การปกปองความเปนสวนตัวของผูใชและขอมูลสวนบุคคลจากการถูกเขาถึงโดยไมไดรับอนุญาต
* การปฏิบัติตามกฎหมายและระเบียบขอบังคับที่เกี่ยวของกับการคุมครองขอมูลสวนบุคคล
* การปฏิบัติตามกฎหมายและระเบียบขอบังคับที่เกี่ยวของกับการคุมครองขอมูลสวนบุคคล

1. การสื่อสารอยางตรงไปตรงมาและโปรงใส:

การสื่อสารกับผูใชและสาธารณะอยางตรงไปตรงมาเกี่ยวกับคุณลักษณะและขอจํากัดของซอฟตแวร

การเปดเผยขอมูลที่สําคัญตอการตัดสินใจของผูใชและสาธารณะ

1. การสงเสริมความเปนธรรมและการเขาถึงเทคโนโลยี:

การพัฒนาซอฟตแวรที่สามารถเขาถึงไดงายและใชงานไดสําหรับทุกคน ไมวาจะมีความสามารถหรือขอจํากัดทางกายภาพ ใดๆ

การสนับสนุนและสงเสริมความเปนธรรมในการเขาถึงและการใชเทคโนโลยี

1. การคํานึงถึงผลกระทบตอสิ่งแวดลอม:

การพัฒนาซอฟตแวรที่ไมกอใหเกิดผลกระทบทางลบตอสิ่งแวดลอม

การสนับสนุนการใชทรัพยากรอยางมีประสิทธิภาพและการลดการปลอยกาซเรือนกระจก

ใสใจในผลกระทบที่ซอฟตแวรจะมีตอสาธารณะ และสังคม

**กรณีตัวอยาง:**

ทีมพัฒนาของบริษัท B กําลังพัฒนาแอปพลิเคชัน สําหรับการแชรรถ (ride-sharing) เมื่อทําการ ออกแบบแอปพลิเคชัน ทีมไดคํานึงถึงผลกระทบตอ การจราจรและสิ่งแวดลอม โดยเพิ่มฟเจอรที่ สงเสริมการใชรถรวมกันในกลุมเพื่อนบานและการ ลดการใชรถยนตสวนตัว

**Ethic code 3. Judgement (จรรยาบรรณตอการวินิจฉัย**) • **หลักการสําคัญ:**

1. การใชวิจารณญาณอยางมีเหตุผล: 1. การตัดสินใจที่อยูบนพื้นฐานของขอมูลและการวิเคราะหที่ถูกตอง 2. การไมตัดสินใจโดยอิงความรูสึกสวนตัวหรือความเคยชิน
2. ความเปนกลางในการตัดสินใจ: 1. การรักษาความเปนกลางและไมเอียงไปทางใดทางหนึ่ง 2. การพิจารณาทุกทางเลือกอยางเทาเทียมกัน
3. .การพิจารณาผลกระทบของการตัดสินใจ: 1. การคํานึงถึงผลกระทบที่อาจเกิดขึ้นทั้งในระยะสั้นและระยะยาว 2. การประเมินความเสี่ยงและการวางแผนเพื่อจัดการกับความเสี่ยง
4. การยึดมั่นในมาตรฐานวิชาชีพ: 1. การปฏิบัติตามมาตรฐานและแนวทางปฏิบัติที่กําหนดโดยองคกรวิชาชีพ 2. การใชแนวทางที่ไดรับการยอมรับในอุตสาหกรรม

ใชวิจารณญาณที่ดีและเปนกลางในการตัดสินใจทาง วิศวกรรม กรณีตัวอยาง:

วิศวกรซอฟตแวร C ตองตัดสินใจเลือกฐานขอมูลสําหรับ ระบบจัดการรานคาออนไลน มีสองตัวเลือก คือ ฐานขอมูลที่เขาถนัดแตประสิทธิภาพตํ่ากวาและ ฐานขอมูลที่ใหมและมีประสิทธิภาพสูงกวา วิศวกร C ตัดสินใจเลือกฐานขอมูลที่มีประสิทธิภาพสูงกวาแมวา จะตองเรียนรูใหม เพราะเห็นวาเปนประโยชนตอระบบ และผูใชงาน

**Ethic code 4. Client and Employer (จรรยาบรรณตอลูกคาและนายจาง**)

หลักการสําคัญ:

1. การปฏิบัติตามความตองการของลูกคา: 1. การเขาใจและตอบสนองตอความตองการและความคาดหวังของลูกคา 2. การใหบริการที่ตรงตามที่สัญญาและใหคําปรึกษาที่เปนประโยชน
2. ความซื่อสัตยและโปรงใส: 1. การสื่อสารอยางตรงไปตรงมาและไมปกปดขอมูลที่สําคัญ 2. การรายงานสถานะของโครงการอยางถูกตองและตรงไปตรงมา
3. การปกปองผลประโยชนของลูกคาและนายจาง: 1. การดําเนินงานที่ปกปองและเสริมสรางผลประโยชนของลูกคาและนายจาง 2. การหลีกเลี่ยงความขัดแยงทางผลประโยชน
4. การรักษาความลับของขอมูล: 1. การรักษาความลับของขอมูลลูกคาและนายจาง 2. การปฏิบัติตามมาตรฐานและกฎหมายที่เกี่ยวของกับการคุมครองขอมูล

ปฏิบัติตามความตองการของลูกคาและนายจาง อยางซื่อสัตยและเปนธรรม

กรณีตัวอยาง:

บริษัท D รับงานพัฒนาระบบจัดการสินคาคง คลังใหกับลูกคา เมื่อลูกคาตองการปรับเปลี่ยน ฟเจอรบางอยาง วิศวกรซอฟตแวรไดแจงให ลูกคาทราบถึงผลกระทบที่อาจเกิดขึ้นและ ระยะเวลาที่จะตองใชในการปรับเปลี่ยนอยาง ตรงไปตรงมา

**Ethic code 5. Management (จรรยาบรรณตอการบริหารจัดการ)**

หลักการสําคัญ:

1. การวางแผนและการจัดการที่ดี: 1. การวางแผนโครงการอยางมีระบบและเปนขั้นตอน 2. การจัดสรรทรัพยากรอยางมีประสิทธิภาพ
2. การติดตามและการประเมินผล: 1. การติดตามความคืบหนาของโครงการอยางสมํ่าเสมอ 2. การประเมินผลการดําเนินงานและการปรับปรุงแผนตามสถานการณ
3. การสื่อสารที่มีประสิทธิภาพ: 1. การสื่อสารกับทีมงานและผูมีสวนไดสวนเสียอยางชัดเจนและตอเนื่อง 2. การรายงานสถานะและปญหาที่เกิดขึ้นใหผูบริหารทราบ
4. การสรางแรงจูงใจและการพัฒนาทีม: 1. การสรางแรงจูงใจใหกับทีมงานเพื่อใหทํางานไดอยางมีประสิทธิภาพ 2. การสงเสริมการพัฒนาทักษะและความรูของทีมงาน

สงเสริมการจัดการที่ดีและมีจรรยาบรรณในโครงการ วิศวกรรม กรณีตัวอยาง:

ผูจัดการโครงการของบริษัท E ไดวางแผนโครงการ พัฒนาระบบ ERP สําหรับองคกรใหญ โดยมีการกําหนด ระยะเวลาและงบประมาณอยางชัดเจน มีการติดตาม ความคืบหนาและปรับปรุงแผนงานตามสถานการณจริง รวมถึงรายงานความคืบหนาใหกับผูบริหารองคกรทราบ อยางสมํ่าเสมอ

**Ethic code 6. Profession (จรรยาบรรณตออาชีพ)**

หลักการสําคัญ:

1. การรักษามาตรฐานวิชาชีพ: 1. การปฏิบัติตามมาตรฐานและแนวทางปฏิบัติที่กําหนดโดยองคกรวิชาชีพ 2. การสงเสริมมาตรฐานที่สูงขึ้นในวิชาชีพ
2. การพัฒนาความรูและทักษะ: 1. การเรียนรูและพัฒนาความรูและทักษะใหมๆ อยางตอเนื่อง 2. การเขารวมกิจกรรมและการอบรมที่เกี่ยวของกับวิชาชีพ
3. การมีสวนรวมในชุมชนวิชาชีพ: 1. การเขารวมและมีสวนรวมในองคกรวิชาชีพ 2. การแบงปนความรูและประสบการณกับเพื่อนรวมวิชาชีพ
4. การสงเสริมความเปนมืออาชีพ: 1. การปฏิบัติตนอยางมืออาชีพในทุกสถานการณ 2. การสงเสริมความนาเชื่อถือและเกียรติยศของวิชาชีพ

รักษามาตรฐานและเกียรติยศของวิชาชีพ วิศวกรรมซอฟตแวร

กรณีตัวอยาง:

วิศวกรซอฟตแวร F เปนสมาชิกของ IEEE และ ปฏิบัติตามมาตรฐานการพัฒนาซอฟตแวรที่ กําหนดโดย IEEE โดยทุกครั้งที่มีการพัฒนา ซอฟตแวรใหม เขาจะตรวจสอบวามีมาตรฐาน ใดบางที่เกี่ยวของและปฏิบัติตามอยางเครงครัด

**Ethic code 7. Colleagues (จรรยาบรรณตอผูรวมงาน)**

หลักการสําคัญ:

1. การทํางานรวมกัน: 1. การทํางานรวมกับเพื่อนรวมงานอยางมีประสิทธิภาพและมีนํ้าใจ 2. การสงเสริมความรวมมือและการทํางานเปนทีม
2. การเคารพและสนับสนุนเพื่อนรวมงาน: 1. การเคารพความคิดเห็นและแนวคิดของเพื่อนรวมงาน 2. การใหการสนับสนุนและคําปรึกษาเมื่อเพื่อนรวมงานตองการ
3. การแบงปนความรูและประสบการณ: 1. การแบงปนความรูและประสบการณเพื่อสงเสริมการเรียนรูรวมกัน 2. การสนับสนุนการพัฒนาความรูและทักษะของเพื่อนรวมงาน
4. การหลีกเลี่ยงการขัดแยง: 1. การหลีกเลี่ยงการขัดแยงที่ไมจําเปนและการแกไขขอขัดแยงอยางสรางสรรค 2. การรักษาความสัมพันธที่ดีและสรางสรรคกับเพื่อนรวมงาน

ปฏิบัติตอเพื่อนรวมงานดวยความเคารพและ สงเสริมความรวมมือ

กรณีตัวอยาง:

วิศวกรซอฟตแวร G ทํางานในทีมพัฒนาแอป พลิเคชันมือถือ เมื่อพบวาเพื่อนรวมงานใหมยัง ไมคุนเคยกับกระบวนการพัฒนาและเครื่องมือที่ ใช เขาไดเสนอที่จะชวยสอนและใหคําปรึกษา เพื่อใหเพื่อนรวมงานใหมสามารถทํางานไดอยาง มีประสิทธิภาพ

**Ethic code 8. Self (จรรยาบรรณตอตนเอง)**

หลักการสําคัญ:

1. การพัฒนาตนเองอยางตอเนื่อง: 1. การเรียนรูและพัฒนาความรูและทักษะใหมๆ อยางตอเนื่อง 2. การวางแผนการพัฒนาตนเองเพื่อใหมีความรูและทักษะที่ทันสมัย
2. การรักษาสุขภาพและความเปนอยูที่ดี: 1. การดูแลสุขภาพกายและจิตใจใหพรอมสําหรับการทํางาน 2. การสรางสมดุลระหวางชีวิตการทํางานและชีวิตสวนตัว
3. การประเมินและปรับปรุงตนเอง: 1. การประเมินผลการทํางานของตนเองอยางเปนระยะ 2. การปรับปรุงการทํางานและการปฏิบัติตนใหดีขึ้น
4. การมีความรับผิดชอบตอตนเอง: 1. การยอมรับความรับผิดชอบตอการกระทําและการตัดสินใจของตนเอง 2. การรักษาความซื่อสัตยและความเปนมืออาชีพในทุกสถานการณ

พัฒนาความรูและทักษะอยางตอเนื่อง

กรณีตัวอยาง:

วิศวกรซอฟตแวร H เขาเรียนคอรสออนไลนเกี่ยวกับ เทคโนโลยีใหมๆ ทุกป เพื่อพัฒนาความรูและทักษะ ทางเทคนิคใหทันสมัย และนําความรูใหมๆ มาใชใน การพัฒนาซอฟตแวรในงานประจํา