

กฎหมายอาชญากรรมคอมพิวเตอร์ เกี่ยวข้องกับองค์กร

ดร. ครรชิต มาลัยวงศ์

ราชบัณฑิต

1 กันยายน 2551

เนื้อหาคำบรรยาย

- อาชญากรรมคอมพิวเตอร์คืออะไร
- วัตถุประสงค์ของกฎหมาย
- รายละเอียดความผิด
- ความเกี่ยวข้องกับองค์กร
- สรุป

คอมพิวเตอร์ กับ การใช้ในทางที่ผิด



- คอมพิวเตอร์เป็นเครื่องมือที่สำคัญที่ช่วยให้เราปฏิบัติงานและดำเนินงานธุรกิจ, ช่วยเราคิด, ช่วยเราเขียน, และ เป็นเครื่องมือสำหรับนันทนาการ
- แต่คอมพิวเตอร์ก็เหมือนเครื่องมืออันมีประโยชน์อื่น ๆ คืออาจมีผู้นำไปใช้ในทางไม่ถูกต้องก็ได้ เช่น นำไปใช้แพร่ภาพอนาจาร, ก่อความรำยผู้ใช้คอมพิวเตอร์อื่น ๆ, หลอกหลวง, ก่อการรำย, ฯลฯ
- การป้องกัน, ปรามปราม, จับกุม, และ ดำเนินคดีแก่ผู้ใช้คอมพิวเตอร์ในทางที่ทำให้เกิดความเสียหายแก่ผู้อื่นจึงเป็นเรื่องจำเป็น

ตัวอย่างอาชญากรรมคอมพิวเตอร์ทั่วไป

- การฉ้อโกงผ่านระบบซื้อขายอิเล็กทรอนิกส์
- การเจาะเข้าสู่ระบบคอมพิวเตอร์เพื่อโจรกรรมข้อมูล, โปรแกรม, และการแก้ไขข้อมูลของผู้อื่น
- การส่งข้อความและภาพลามกอนาจาร
- การใช้คอมพิวเตอร์ในการล่อลวง-ปัจจุบันเป็นข่าวเสมอ
- การสร้างภาพตัดต่ออันทำให้เกิดความเสียหายแก่ผู้อื่น
- การละเมิดสิทธิส่วนบุคคลของผู้อื่น ทำให้คอมพิวเตอร์ของผู้อื่นเสียหาย



การดำเนินงานของไทย

- เนกเทค ในฐานะ สำนักงานเลขานุการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ได้ผลักดันเรื่องนี้มานานแล้ว โดยได้ตั้งสำนักงานย่อยเพื่อประสานงานในการร่างกฎหมายที่เกี่ยวกับไอทีหลายฉบับ
 - พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
 - พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
 - กฎหมายข้อมูลส่วนบุคคล
 - กฎหมายบัตรเครดิต
 - กฎหมายการโอนเงินทางอิเล็กทรอนิกส์
 - ฯลฯ



๒. แนวทางในการยกร่างกฎหมาย Cybercrime Convention ของ Council of Europe

กลุ่มประเทศ	ร่วมลงนาม	ให้สัตยาบัน
สมาชิก Council of Europe	๔๖ ประเทศ	๑๘ ประเทศ
ประเทศซึ่งไม่ใช่ สมาชิก Council of Europe	๗ ประเทศ แคนาดา เม็กซิโก สหรัฐอเมริกา ญี่ปุ่น มอนเตเนโกร คอซตาริกา แอฟริกาใต้	๑ ประเทศ สหรัฐอเมริกา
รวม	๕๓ ประเทศ	๑๙ ประเทศ

Source : <http://conventions.coe.int/> ข้อมูล ณ วันที่ ๗ พฤษภาคม ๒๕๕๐⁶

พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

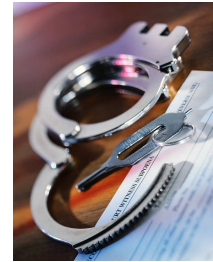
- ประกาศในราชกิจจานุเบกษาเมื่อ ๑๘ มิ.ย. ๕๐
- บังคับใช้ ๑๘ กรกฎาคม ๒๕๕๐
- ประกอบด้วยสองหมวด ๓๐ มาตรา
- หมวดที่ ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ มี ๑๓ มาตรา
- หมวดที่ ๒ พนักงานเจ้าหน้าที่ มี ๑๓ มาตรา
- ต่อมามีการประกาศวิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งมีผลใช้บังคับ 23 สิงหาคมนี้



เจตนาารมณ์ของกฎหมาย

เพื่อกำหนด...

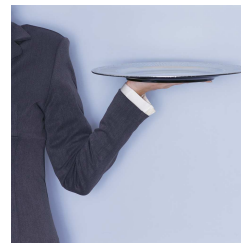
- ฐานความผิดและบทลงโทษ



- อำนาจหน้าที่ของพนักงานเจ้าหน้าที่



- หน้าที่ของผู้ให้บริการ



หมวดที่ ๑

มาตรา ๕ การไปเปิดคอมพิวเตอร์ของคนอื่นโดยใช้ password ของเขาโดยไม่ได้รับอนุญาต มีความผิดระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ เอา Password ของคนอื่นไปบอกแก่บุคคลที่สาม ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

หมวดที่ ๑

มาตรา ๗ การเปิดอ่านหรือแก้ไขข้อมูลคอมพิวเตอร์ของคนอื่นซึ่งมีการป้องกัน และไม่ได้ให้เราใช้ แม้จะอยู่ในคอมพิวเตอร์ของเรา ก็ผิด และ ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ การ**ดักจับอีเมล** หรือ **การส่ง ข้อมูล** คอมพิวเตอร์ของผู้อื่นที่และข้อมูลคอมพิวเตอร์นั้นไม่ได้ให้บุคคลทั่วไปใช้ต้องระวางโทษจำคุกไม่เกิน ๓ ปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

หมวดที่ ๑

มาตรา ๘ ผู้ใด**ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือ เพิ่มเติม** ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกิน ห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ การทำให้ **การทำงานของระบบ คอมพิวเตอร์ของผู้อื่นไม่** สามารถทำงานตามปกติได้ เช่น การปล่อยไวรัสรบกวน, การส่งหนอน, การเปลี่ยนหน้าเว็บของคนอื่น ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

หมวดที่ ๑

มาตรา ๑๑ ผู้ใดส่งสแปมเมล หรือ จดหมายลูกโซ่อัน

เป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ เพิ่มโทษหากกระทำความผิดตามมาตรา ๙ หรือ ๑๐ และ

ก่อให้เกิด ความเสียหายแก่ประชาชน หรือ ต่อข้อมูลคอมพิวเตอร์

หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัย

ของประเทศ จนถึงกับทำให้มีผู้เสียชีวิต ฯลฯ

หมวดที่ ๑

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่โปรแกรมเพื่อนำไปใช้เป็น
เครื่องมือในการกระทำความผิดตามมาตรา ๕ ถึง ๑๑ ต้องระวาง
โทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำ
ทั้งปรับ



หมวดที่ ๑

มาตรา ๑๔ การนำข้อมูลปลอมหรือเป็นเท็จทำให้เกิดความเสียหายหรือประชาชนตื่นตระหนก รวมทั้งการก่อการร้าย และ ข้อมูลลามกอนาจาร ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

หมวดที่ ๑

มาตรา ๑๕ การสนับสนุนหรือยินยอมให้มีการกระทำผิดตาม มาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้อง ระวังโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ประเด็นนี้ผู้บริหารหรือหัวหน้าต้องระมัดระวัง และ สร้างแนวทาง ในการควบคุมการทำงานของพนักงาน



หมวดที่ ๑

มาตรา ๑๖ การตัดต่อภาพของผู้อื่น จนทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือ ปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ
(หากทำโดยสุจริต ผู้กระทำไม่มีความผิด, เป็นความผิดที่ยอมความกันได้)



หมวดที่ ๑

มาตราที่ ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอก
ราชอาณาจักรและ

- (๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่
ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ
 - (๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือ
คนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ
- จะต้องรับโทษภายในราชอาณาจักร



การเจาะเข้าสู่ระบบโดยแฮกเกอร์

ความเป็นมาของการเจาะระบบ

- ยุคแรก ๆ
 - มีมานานแล้วคือตั้งแต่ราวปี 1960s
 - ในช่วงแรก ๆ นั้นผู้เป็นแฮกเกอร์มักจะเป็นนักโปรแกรมที่มีความสามารถในการเขียนโปรแกรม
 - ระบบปฏิบัติการและเกมคอมพิวเตอร์แรก ๆ นั้นเขียนโดยบรรดาแฮกเกอร์
 - ในช่วงแรกคำว่าแฮคกิงมีความหมายในทางที่ดี น่าชื่นชม
 - ต่อมาแฮกเกอร์มักจะเป็นนักศึกษาและนักเรียน



การเจาะเข้าสู่ระบบโดยแฮกเกอร์



แฮกเกอร์ในยุคอินเทอร์เน็ต

- เริ่มมาราวสิบกว่าปีแล้ว เมื่อมีการใช้อินเทอร์เน็ตอย่างกว้างขวางทั้งทางด้านการศึกษา, ธุรกิจ และ ตามบ้านเรือน ทำให้บรรดาอาชญากรเริ่มสนใจ
- อาชญากรรมแรก ๆ คือการปล่อยไวรัสและหนอน
- คอมพิวเตอร์ที่ไม่มีการป้องกันที่ดีอาจมีคนแอบใช้เพื่อก่อความเดือดร้อนแก่ผู้อื่น, รวมทั้งการใช้ในการหลอกลวง, และการทำให้ระบบเครือข่ายเสียหาย
- แฮกเกอร์ไม่จำเป็นต้องเก่ง เพราะอาจใช้โปรแกรมที่คนอื่นเขียนไว้ไปสร้างความเดือดร้อนได้

คำใหม่ - Hacktivism

- หมายถึง การใช้ประสบการณ์ในการเจาะระบบเพื่อสนับสนุนงานการเมือง
 - การเจาะระบบแบบนี้อาจเป็นกิจกรรมการสร้างปัญหาที่ร้ายแรง
 - Hacktivism เป็นการต่อต้านสังคมในรูปแบบใหม่ของยุคปัจจุบัน
 - Hacktivism เป็นการปฏิเสธสิทธิในการแสดงความคิดเห็นของบุคคลอื่น และ ละเมิดสิทธิในทรัพย์สินทางปัญญาของผู้อื่น



กฎหมายป้องกันใน สรอ.

- **Computer Fraud and Abuse Act (CFAA, 1986)**
 - It is a crime to access, alter, damage, or destroy information on a computer without authorization.
 - Computers protected under this law include:
 - government computers,
 - financial systems,
 - medical systems,
 - interstate commerce, and
 - any computer on the Internet.

กฎหมายป้องกันใน สรอ.

- The Law (cont'd)
 - USA Patriot Act (USAPA, 2001)
 - Amends the CFAA.
 - Allows for recovery of losses due to responding to a hacker attack, assessing damages, and restoring systems.
 - Higher penalties can be levied against anyone hacking into computers belonging to criminal justice system or the military.
 - The government can monitor online activity without a court order.

Hacking

- **การจับกุมแฮกเกอร์**
 - จำเป็นต้องใช้เจ้าหน้าที่ที่มีความรู้ความชำนาญ, ตรวจพบว่ามีการเจาะระบบ และ ดำเนินการสอบสวนจับกุม
 - การสืบสวนสอบสวนต้องใช้เครื่องมือเช่น :
 - สายสืบ
 - บันทึกข้อมูลการใช้กระดานข่าว, จุดหมายอิเล็กทรอนิกส์
 - เครื่องมือสำหรับกู้ข้อมูลที่ถูกลบทิ้งแล้ว
 - เครื่องมือสำหรับถอดรหัส
 - บันทึกข้อมูลจราจร หรือ การใช้คอมพิวเตอร์ผ่านระบบเครือข่าย และ ผู้ให้บริการเครือข่าย
 - วิชาการสำคัญเรียกว่า **Computer Forensics**



ปัญหาแง่คิดทางกฎหมาย



■ เจตนา

- ศาลควรลงโทษผู้ที่กระทำความผิดที่ไม่ต้องการสร้างความเสียหายหรือก่อให้เกิดอันตรายแตกต่างไปจากผู้กระทำความผิดที่เป็นอาชญากรและมีเจตนาสร้างความเสียหายจริงหรือไม่?

■ อายุ

- ผู้กระทำความผิดที่อายุน้อยควรได้รับโทษแตกต่างจากผู้ที่มีอายุมากกว่าหรือไม่?

■ ความเสียหายที่เกิดขึ้น

- การลงโทษหนักเบาควรขึ้นกับความรุนแรงของความเสียหายที่เกิดขึ้นหรือไม่?

ปัญหาแง่คิดทางกฎหมาย



- การทำผิดนอกประเทศ หรือ โดยคนต่างด้าว
 - จะมีวิธีการดำเนินการอย่างไร
- การบล็อกเว็บโดยหน่วยงาน เช่น ก. ไอซีที
 - ยังจำเป็นหรือไม่
- การตรวจสอบเว็บของพนักงาน
 - จะทำได้หรือไม่

ปัญหาแง่คิดทางกฎหมาย

- การนำรูปการ์ตูน นายกฯ สมัคร ที่เขียนล้อการเมืองมาลงไว้ในเว็บจะผิดกฎหมายหรือไม่ เพราะเหมือนกับการดัดแปลงภาพ
- รูปการ์ตูนสนุก ๆ ที่มีรูปโป๊ จะเป็นรูปลามกอนาจารหรือไม่
- ถ้าหากการจัดเก็บ **Log** เป็นไปตามระเบียบ แต่ Log ของวันนั้นเกิดความเสียหายเพราะเครื่อง **crash** และต้องใช้ **log** นั้นพอดี จะเกิดความผิดหรือไม่

ข้อเสนอแนะ

- บริษัทในเครือส่วนมากเวลานี้ได้ให้หมายเลขอีเมลแก่พนักงานอยู่แล้ว ดังนั้นจึงควร
 - ทบทวนและให้หมายเลขให้ครบ อย่าให้หลายคนใช้หมายเลขเดียว
 - จัดวิธีทำ **authentication**
 - จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เอาไว้ครบ **90** วัน
 - เผยแพร่นโยบาย และ ห้ามปรามไม่ให้พนักงานทำผิด
 - รีบจัดทำนโยบายความมั่นคงคอมพิวเตอร์

เหตุใดเราจึงถูกเจาะระบบได้

■ ความมั่นคง

- คอมพิวเตอร์ของหน่วยงานส่วนใหญ่มีจุดอ่อนด้านการรักษาความมั่นคง:
 - ขาดการตระหนักถึงปัญหา ทำให้ไม่มีการป้องกัน
 - การป้องกันไม่พอเพียงเพราะขาดงบประมาณ
 - ไม่มีระเบียบปฏิบัติที่รัดกุม
 - ไม่ได้แนะนำและให้ความรู้แก่พนักงาน
- สาเหตุของจุดอ่อน
 - ธรรมชาติของอินเทอร์เน็ตกับเว็บ
 - ธรรมชาติของคนที่ต้องการระบายความโกรธ
 - ความซับซ้อนของระบบคอมพิวเตอร์



การป้องกันการเจาะระบบ

- พยายามให้ความรู้และความเข้าใจแก่พนักงานทุกคน
- ออกแบบระบบให้มีการเตือนและป้องกัน
- ใช้ระบบและเครื่องมือป้องกัน
- ติดตามข่าวสารการแพร่โปรแกรมไวรัสที่มีหน่วยงานสาธารณะคอยตรวจสอบ
- กำหนดให้มีการแจ้งปัญหาที่น่าสงสัยว่าจะเป็นไวรัส หรือ มีการบุกรุก



ความครอบคลุมของกฎหมายไทย

- เท่าที่พิจารณาจากมาตราต่าง ๆ และจากการเจาะระบบของแฮกเกอร์ เชื่อว่า พรบ. ฉบับนี้ ครอบคลุมการกระทำผิดด้านนี้ค่อนข้างดีแล้ว



อาชญากรรมออนไลน์

- **การประมูลซื้อขายสินค้าทางอินเทอร์เน็ต**
 - ปัจจุบันการซื้อขายสินค้าแบบออนไลน์ได้รับความนิยมมาก
 - ปัญหา
 - ผู้ขายไม่ส่งสินค้าให้
 - ผู้ขายส่งสินค้าที่ด้อยคุณภาพมาให้
 - ราคาสูงเกินสมควรเพราะมีการแข่งขัน
 - มีการขายสินค้าผิดกฎหมาย
 - วิธีการแก้ไข
 - ให้คำแนะนำแก่ผู้สนใจซื้อสินค้าแบบออนไลน์
 - อ่านข้อมูลของผู้ขายอย่างละเอียด
 - ซื้อขายผ่านบุคคลที่สาม
 - ฯลฯ



การฉ้อโกง, หลอกหลวง และ การบ่อนทำลาย

- **ตัวการที่ทำให้เกิดการฉ้อโกง**
 - **บัตรเครดิต**
 - ใบเสร็จรับเงินถูกขโมย, เอกสารรายงานการเงิน, บัตร
 - การดักจับข้อมูลออนไลน์ หรือ ระบบความมั่นคงของการพาณิชย์อิเล็กทรอนิกส์ที่มีจุดอ่อน
 - เจ้าของบัตรเดินเล่อ
 - **ATM**
 - การขโมยหมายเลขบัตรและ PINs.
 - ข้อมูลวงใน
 - การปลอมบัตร ATM
 - **ระบบโทรคมนาคม**
 - การขโมย PINs ผ่านระบบสื่อสาร.
 - การใช้โทรศัพท์หลอกหลวง
 - Phishing



ความครอบคลุมของกฎหมายไทย

- ยังไม่แน่ใจในเรื่องเหล่านี้ เพราะมีการฉ้อโกงที่ลึกซึ้งมากขึ้นทุกวัน
- การฟ้องร้องอาจต้องใช้กฎหมายอื่นเข้ามาประกอบ



ความเกี่ยวข้องกับองค์กร

- หน่วยงานที่ให้บริการเว็บ, อีเมล, บล็อก ล้วนเกี่ยวข้องกับโดยตรง
- ต้องปฏิบัติตามกฎหมายไม่มีข้อยกเว้น
- ตย. สถานศึกษามีฐานะเป็นผู้ให้บริการด้วย ดังนั้น จึงต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์เอาไว้ให้ตรวจสอบ
- ต้องสร้างความเข้าใจแก่บุคลากรเพื่อไม่ให้ทำผิดกฎหมาย
- ต้องดูแลอย่าให้เกิดการกระทำผิดกฎหมาย
- ต้องมีระบบตรวจสอบความมั่นคงด้วย



องค์ประกอบสำคัญของความมั่นคง

- ความมั่นคงทางการบริหารและขององค์กร
- ความมั่นคงปลอดภัยของบุคลากร
- ความมั่นคงทางกายภาพ
- ความมั่นคงของระบบสื่อสาร
- ความมั่นคงของฮาร์ดแวร์และซอฟต์แวร์
- ความมั่นคงของการปฏิบัติการ
- การวางแผนฉุกเฉิน



หมวดที่ ๒ พนักงานเจ้าหน้าที่

กำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่และหน้าที่ของผู้ให้บริการ	
มาตรา ๑๘	อำนาจของพนักงานเจ้าหน้าที่
มาตรา ๑๙	การตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่
มาตรา ๒๐	การใช้อำนาจในการ block เว็บไซต์ที่มีเนื้อหากระทบต่อความมั่นคงหรือขัดต่อความสงบเรียบร้อย
มาตรา ๒๑	การห้ามเผยแพร่/จำหน่ายชุดคำสั่งไม่พึงประสงค์
มาตรา ๒๒	ห้ามมิให้พนักงานเจ้าหน้าที่เผยแพร่ข้อมูลที่ได้มาตรา ๑๘
มาตรา ๒๓	พนักงานเจ้าหน้าที่ประเภทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูล
มาตรา ๒๔	ความรับผิดของผู้ล่วงรู้ข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และนำไปเปิดเผย
มาตรา ๒๕	ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ
มาตรา ๒๖ ถึง ๒๗	หน้าที่ผู้ให้บริการในการเก็บข้อมูลจราจรทางคอมพิวเตอร์และความรับผิด หากไม่ปฏิบัติตามหน้าที่
มาตรา ๒๘	การแต่งตั้งพนักงานเจ้าหน้าที่
มาตรา ๒๙	การรับคำร้องทุกข์กล่าวโทษ จับ ควบคุม ค้น & การกำหนดระเบียบ/แนวทางและวิธีปฏิบัติ
มาตรา ๓๐	การปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่
รวมทั้งสิ้น ๑๓ มาตรา	

การตรากฎกระทรวง & ประกาศ/ระเบียบ

กฎกระทรวงกำหนดหนังสือยึดหรืออายัดระบบคอมพิวเตอร์ (มาตรา ๑๙)

- ประกาศห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ (มาตรา ๒๑)
- การจัดทำประกาศเกี่ยวกับผู้ให้บริการและข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา ๒๖)
- การจัดทำประกาศเกี่ยวกับการกำหนดคุณสมบัติพนักงานเจ้าหน้าที่ (มาตรา ๒๘)
- การจัดทำประกาศเกี่ยวกับบัตรประจำตัวพนักงานเจ้าหน้าที่ (มาตรา ๓๐)

การจัดทำระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดี (มาตรา ๒๙)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

วัตถุประสงค์ ออกภายใต้ ม.๒๖ วรรค ๓ เพื่อกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อเป็นพยานหลักฐานสำคัญต่อการนำตัวผู้กระทำความผิดมาลงโทษ

ประเภทผู้ให้บริการ แบ่งเป็น ๒ ประเภทใหญ่

(๑.) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ตหรือให้สามารถติดต่อถึงกัน โดยประการอื่น ทั้งนี้โดยผ่านทางระบบคอมพิวเตอร์ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๕ ประเภท ดังนี้

- ผู้ประกอบกิจการ โทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)
- ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)
- ผู้ให้บริการเช่าระบบคอมพิวเตอร์หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider)
- ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒.) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่าง ๆ (Application Service Provider)

ข้อมูลที่ต้องเก็บ

เก็บข้อมูลจราจรที่ สามารถระบุผู้ใช้บริการเป็นรายบุคคลได้

รูปแบบการเก็บ

ต้องเก็บในสื่อที่รักษา Integrity/identification/Confidentiality

บทเฉพาะกาล

เริ่มเก็บ ๓๐ วัน/๕๐ วัน/๑ ปี นับจากวันประกาศในราชกิจจานุเบกษา

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

วัตถุประสงค์ ออกภายใต้ มาตรา ๒๘ เพื่อให้การแต่งตั้งพนักงานเจ้าหน้าที่ที่มีความชัดเจนและมีการปฏิบัติหน้าที่เป็นไปอย่างมีประสิทธิภาพ

พนักงานเจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แบ่งเป็น

คุณสมบัติ

- มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์
- สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรี ทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์
- ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) สอบสวน สอบสวน และการพิสูจน์ หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ตามภาคผนวกท้ายประกาศนี้ และ
- มีคุณสมบัติอื่นอย่างหนึ่งอย่างใดตามประกาศ

ระยะเวลา

ดำรงตำแหน่งในวาระคราวละ ๔ ปี ตามประกาศในราชกิจจานุเบกษา

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง แต่งตั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

วัตถุประสงค์ อาศัยอำนาจตามความในมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ. ๒๕๕๐

รายชื่อพนักงานเจ้าหน้าที่

- นายวรพัฒน์ ทิวถนอม
- นายอาจิน จิรัชพัฒนา
- นายวินัย อยู่สบาย
- นายธนิต ประภาคนันท์
- นายอารีย์ จิวรักษ์
- นายสมศักดิ์ ศุภจิราวัฒน์
- นายสุรชัย นิลแสง
- นายณัฐวุฒิ ภัทรประยูร
- นายไพรัช อิงคสิทธิ์
- นายสมญา พัฒนารพันธ์
- นายจิโรภาส พูลสุวรรณ
- นายทรงกลด ป่าเจริญ
- นายอิทธิฤทธิ์ ไชยจันทร์
- พันตำรวจโท วิวัฒน์ สิริสรเดช
- พันตำรวจโท อัยฉ่างค์ ม่วงศรี

หมายเหตุ ยังมีการประกาศรายชื่อพนักงานเจ้าหน้าที่นอกเหนือจากนี้อีก แต่ไม่ได้นำมาลงไว้

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

แบบบัตรประจำตัวพนักงานเจ้าหน้าที่

ด้านหน้า

ติดรูปถ่าย ขนาด 2.5 X 3 ซม.	ชื่อ.....	เลขที่.....
	Name.....	
	หน่วยงาน.....	
	เลขประจำตัวประชาชน.....	
	ตำแหน่ง.....	
ลายมือชื่อผู้ถือบัตร	ผู้ถือบัตร	
	วันออกบัตร...../...../.....	บัตรหมดอายุ...../...../.....

กว้าง 5.4 ซม.
ยาว 8.5 ซม.

ด้านหลัง

แอบแม่เหล็ก
บัตรประจำตัวพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทางเดินบัตรนี้ได้ถูกดัดแปลงเพื่อวัตถุประสงค์และใช้สำหรับ พริอ โพร. ๑๑๑

สรุป

- พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็น กฎหมายสำคัญที่ ได้รับการตราขึ้นเพื่อช่วยให้การดำเนินงานด้านคอมพิวเตอร์ปราศจากปัญหา, สังคมเกิดสันติสุข, และ ประเทศเป็นที่ยอมรับในสังคมโลก
- การปฏิบัติตามพระราชบัญญัติเป็นหน้าที่ของทุกคน
- ปัญหาสำคัญคือพนักงานเจ้าหน้าที่ จะดำเนินการตรวจสอบการใช้คอมพิวเตอร์ให้ เป็นไปตามกฎหมายได้มากน้อยเพียงใด และ จะมีเวลาอุทิศให้กับการ ปราบปรามการกระทำผิดได้เพียงใด

