แนวทางการปฏิบัติ และ สรุปรายละเอียด
พระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เอกสารฉบับนี้สรุปเนื้อหาจาก 1) พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (พรบ.ความผิดคอมพิวเตอร์ 2550) และ 2) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลทางจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (ประกาศ ICT) ซึ่งคัดเฉพาะส่วนที่มีผลบังคับใช้กับผู้ดูแลและผู้ใช้งานระบบและเครือข่ายคอมพิวเตอร์ของคณะวิทยาศาสตร์ทุกท่าน เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็น ส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบ คอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือ ใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือ ใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิด ความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรม อันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

1. คำแนะนำวิธีปฏิบัติ ตาม พรบ. ความผิดคอมพิวเตอร์ 2550

- ไม่ตัดต่อเผยแพร่ภาพตัดต่อของผู้อื่น ที่ทำให้เขาเสียหายหรือเสียชื่อเสียง
- ก่อนดาวโหลดโปรแกรมหรือข้อมูลจากเว็บไซต์ ควรอ่านเงื่อนไขให้ละเอียดเสียก่อน
- ไม่ฟอร์เวิร์ดอีเมล์ หรือ Clip ภาพลามกอนาจาร หรือข้อความไม่เหมาะสม
- ไม่เผยแพร่ Spam mail หรือไวรัส
- ไม่เปิดเผยมาตรการระบบคอมพิวเตอร์ให้ผู้อื่นล่วงรู้
- ไม่ขโมยข้อมูลระบบคอมพิวเตอร์ของผู้อื่น
- ระวังการ Chat กับคนแปลกหน้า อย่าหลงเชื่อเขาง่ายๆ
- อย่าลืม ลงโปรแกรมป้องกันไวรัสและสปายแวร์
- ไม่แฮกระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่น
- ไม่ควรบันทึก Password ไว้ในเครื่องคอมพิวเตอร์และควรเปลี่ยน Password ทุกๆ 3 เดือน
- ไม่แอบดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น
- ไม่นำเข้าข้อมูลหรือภาพลามก อนาจาร เข้าไปในระบบคอมพิวเตอร์

2. สรุป เนื้อหาพรบ.ความผิดคอมพิวเตอร์ 2550 และประกาศ ICT

การกระทำที่ถือว่าเป็นความผิดตามพรบ. (สำหรับผู้ใช้งาน)

1. การล่วงล้ำเข้าไปในระบบคอมพิวเตอร์ หรือ ข้อมูลคอมพิวเตอร์ (เช่นหน้าเวบ หรือ directory/folder) ของผู้อื่นที่มีมาตรการป้องกันไว้โดยเฉพาะ รวมถึงหากผู้ที่ทราบมาตรการการป้องกันนำมาตรการที่ล่วงรู้มาไปเผยแพร่

2. การดักจับข้อมูลของผู้อื่นที่อยู่ระหว่างการสื่อสาร
3. การทำลาย แก้ไข หรือเปลี่ยนแปลงข้อมูลของผู้อื่นโดยมิชอบ
4. การกระทำการใดๆเพื่อทำให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ หรือถูกรบกวน
5. การส่งข้อมูลคอมพิวเตอร์หรือ Email ที่ปกปิด/ปลอมแปลงที่มาของข้อมูล (spam mail) ที่เป็นการรบกวนผู้อื่น
6. การนำข้อมูลไม่เหมาะสมเข้าสู่ระบบคอมพิวเตอร์ ซึ่งทำให้เกิดความเสียหายต่อประชาชนและประเทศ ตัวอย่างข้อมูลไม่เหมาะสมได้แก่: ข้อมูลปลอม, ข้อมูลอันเป็นเท็จ, ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงของประเทศ, และภาพลามก
7. การเผยแพร่หรือส่งต่อข้อมูลที่ไม่เหมาะสมดังกล่าว
8. การยอมให้ผู้อื่นบรรจุข้อมูลที่ไม่เหมาะสม ลงบนระบบคอมพิวเตอร์ที่ตนรับผิดชอบ
9. การสร้าง ตัดต่อ ดัดแปลงภาพของผู้อื่น ที่ทำให้ผู้อื่นเสียหาย หรืออับอาย
10. การเผยแพร่ software ที่เป็นเครื่องมือในการทำผิดตามข้อ1ๆ

ข้อปฏิบัติ สำหรับผู้ดูแลระบบ

1. ไม่สนับสนุนหรือยินยอมให้ผู้ใช้บริการนำเข้า หรือเผยแพร่ข้อมูลที่ไม่เหมาะสมเขาไปในระบบคอมพิวเตอร์
2. ระงับการเผยแพร่เว็บไซต์ที่มีข้อมูลกระทบกระเทือนต่อความมั่นคง ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี
3. ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการดำเนินการสืบสวน สอบสวน หาตัวผู้กระทำผิด
4. ผู้ให้บริการจะต้องเก็บข้อมูลการจราจรทางคอมพิวเตอร์ที่อยู่ภายใต้ความรับผิดชอบไว้อย่างน้อย 90 วัน
5. ข้อมูลที่จัดเก็บจะต้องได้รับการปกป้องให้มีความน่าเชื่อถือ และไม่ถูกเปลี่ยนแปลงได้จากผู้ใช้และผู้ดูแลระบบ การเข้าถึงข้อมูล (แต่ห้ามเปลี่ยนแปลง) จะกระทำได้โดยผู้ที่ได้รับมอบหมายเท่านั้น
6. ข้อมูลที่เก็บนั้น จะต้องครอบคลุมการเข้าใช้งานเครือข่ายคอมพิวเตอร์ในทุกรูปแบบ (เช่นทั้ง wired และ wireless) และจะต้องสามารถระบุตัวผู้ใช้บริการเป็นรายบุคคลได้จริง
7. ผู้ให้บริการต้องตั้งเวลาของอุปกรณ์ทุกชนิดให้ตรงกับสากล โดยผิดพลาดไม่เกิน 10 มิลลิวินาที
8. ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องจัดเก็บคือ

- **การเข้าถึงระบบเครือข่าย:** User ID, วันเวลาการเข้าใช้งาน, IP Address ของเครื่องที่ใช้, และหมายเลขสายที่เรียกเข้า (เช่น กรณี Modem หรือ ADSL)
- **E-Mail:** Message ID, Email ของผู้รับและผู้ส่ง, วันเวลาการติดต่อและใช้งาน, IP Address ของเครื่องที่เข้ามาใช้งาน, User ID ของผู้ใช้งาน (ถ้ามี), POP3/IMAP4 Log
- **File Transfer/File Sharing:** วันเวลาการเข้าใช้งาน, IP Address ของเครื่องผู้ใช้, User ID (ถ้ามี), path และ file name
- **Web Server:** วันเวลาการติดต่อ, IP Address ของเครื่องผู้ใช้, คำสั่งการใช้งานเวบ, URI (หน้าเวบที่เรียกใช้)
- **Instant Messaging (เช่น MSN):** วันเวลาการติดต่อ, IP Address ของผู้ใช้

บทกำหนดโทษ

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา ๕ เข้าถึงระบบคอมพิวเตอร์ ที่มีการป้องกันโดยมิชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
มาตรา ๖ ล่วงรู้และเผยแพร่มาตรการป้องกัน	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๗ เข้าถึงข้อมูลคอมพิวเตอร์ ที่มีการป้องกันโดยมิชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
มาตรา ๘ การดักข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๙ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๐ การรบกวนระบบคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๑ ส่งข้อมูล หรือ E-Mail ที่ปกปิดแหล่งที่มา และเป็นการรบกวนผู้อื่น	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๒ หากการกระทำ ข้อ ๙ และ ข้อ ๑๐ (๑) ก่อความเสียหายแก่ประชาชน ทั้งทันทีและภายหลัง (๒) กระทบต่อความมั่นคงปลอดภัยประเทศ/เศรษฐกิจถ้าเป็นเหตุให้เสียชีวิต	ไม่เกิน ๑๐ ปี ๓ ถึง ๑๕ ปี ๑๐ ถึง ๒๐ ปี	ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐ – ๓๐๐,๐๐๐ บาท ไม่มี
มาตรา ๑๓ การจำหน่าย/เผยแพร่ Software ที่ใช้กระทำผิด	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๑๔ เผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๕ ISP ที่ยอมให้เผยแพร่ข้อมูลที่ไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๖ การตัดต่อภาพผู้อื่น และทำให้เสียหาย *(ถ้าสุจริต หรือไม่เสียหาย ไม่มีความผิด)*	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท