แนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ กรมพัฒนาที่ดิน

อริศรา พึ่งพา
นักวิชาการคอมพิวเตอร์ชำนาญการ
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
e-Mail : arissara.p@ldd.mail.go.th

หลักการเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 มาตรา 6 และมาตรา 9 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

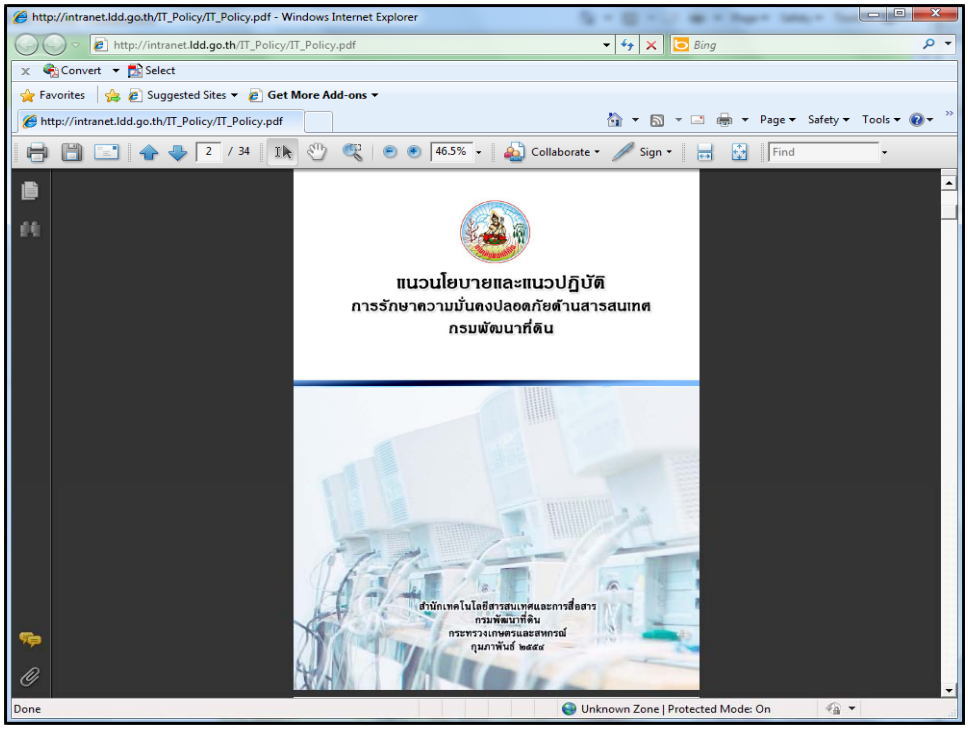
วัตถุประสงค์

1. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและปฏิบัติได้อย่างถูกต้องตากกฎหมายต่าง ๆ ที่เกี่ยวข้องได้กำหนดไว้
2. เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

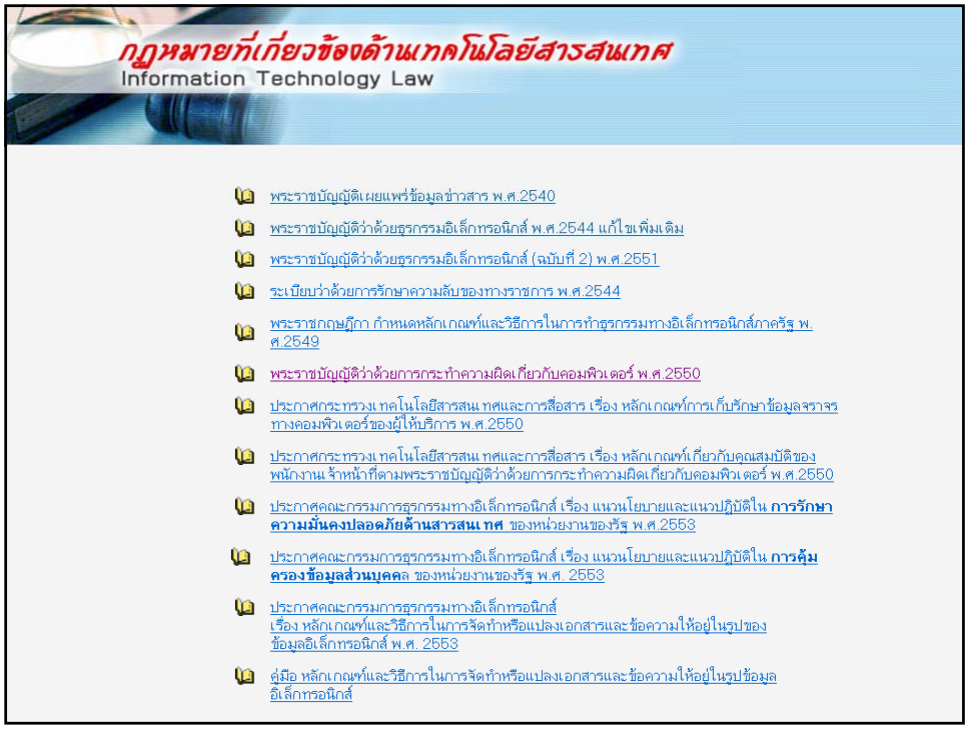
วัตถุประสงค์

3. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้ผู้บริหารเจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
4. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้ง ต่อปี


LDD Intranet
Land Development Department
การบริหารความเสี่ยง กรมพัฒนาที่ดิน
การบริหารความเสี่ยง ด้านระบบเทคโนโลยีสารสนเทศ (IT Risk Management)
แนวนโยบายและแนวปฏิบัติ การรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ กรมพัฒนาที่ดิน
แผนรับสถานการณ์ฉุกเฉิน จากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan)
ระเบียบปฏิบัติและคู่มือด้านสารสนเทศ
พระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
รวมกฎหมายที่เกี่ยวข้อง ด้านเทคโนโลยีสารสนเทศ
ระเบียบการใช้งานบนระบบเครือข่าย
คู่มือการใช้งานบนระบบเครือข่าย
คู่มือการใช้งานระบบการประชุมอิเล็กทรอนิกส์ (e-meeting) สำหรับผู้ใช้งานทั่วไป
บุคลากรด้าน IT
หัวหน้ากลุ่มประสานงานและเจ้าหน้าที่ด้าน IT
รายชื่อผู้รับผิดชอบระบบการประชุมทางไกล (Video Conference)
ข่าวประชาสัมพันธ์
สามารถดูเนื้อหา พ.ร.บ. คอมพิวเตอร์ 2550 http://www.ldd.go.th/web_Enactment/
สามารถดูเนื้อหาของกฎหมายได้ที่ http://intranet.ldd.go.th/Information_Law/index.html
โครงข่ายอัจฉริยะ กรมพัฒนาที่ดิน
ระบบบริการส่งข้อความสั้น (SMS)
สารสนเทศทรัพยากรบุคคล (DPIS)
ไปรษณีย์ พ.ด. LDD Mail
E-Mail Address
ระบบการประชุมอิเล็กทรอนิกส์ e-Meeting
สำนักงานอิเล็กทรอนิกส์ e-Office
สารบรรณและตู้เอกสารอิเล็กทรอนิกส์
การเงิน/สหกรณ์
คำสั่งต่าง ๆ
ฟอนต์มาตรฐานไทย
ฐานข้อมูลครุภัณฑ์สิ่งก่อสร้าง
คำสาธารณูปโภค


http://intranet.ldd.go.th/IT_Policy/IT_Policy.pdf - Windows Internet Explorer
แนวนโยบายและแนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมพัฒนาที่ดิน
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
กรมพัฒนาที่ดิน
กระทรวงเกษตรและสหกรณ์
กุมภาพันธ์ ๒๕๕๔
Done
Unknown Zone | Protected Mode: On


พระราชบัญญัติว่าด้วยการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
พรบ.คอมพิวเตอร์ พ.ศ.2550
สอบถามรายละเอียดเพิ่มเติมได้ที่
ระบบล็อกอิน(Login) การเชื่อมต่ออินเทอร์เน็ต
เริ่มใช้งานตั้งแต่วันที่ 22 สิงหาคม 2551 เวลา 16.30 น. Download!
คู่มือ การจัดเก็บ Log File ของเครื่อง Server ของ สพธ. ที่ให้บริการ Download!
รายชื่อผู้รับมอบหมายการเก็บ Log File สำนักงานพัฒนาที่ดิน เขต 1-12
รายละเอียดเกี่ยวกับพระบัญญัติคอมพิวเตอร์
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 Download!
แผนผังพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 Download!
แผ่นปลิวพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 Download!
บันทึกข้อความ
บันทึกข้อความ เรื่อง ข้อปฏิบัติเกี่ยวกับการขึ้นทะเบียนคอมพิวเตอร์และการยืนยันตัวบุคคล Download!
บันทึกข้อความ เรื่อง การมีกฎปฏิบัติการเก็บ Log File Server ที่ให้บริการของ สพธ. และ GIS Web Server Download!
แบบฟอร์มและวิธีการเช็คข้อมูลในแบบฟอร์ม
แบบฟอร์มการขึ้นทะเบียนคอมพิวเตอร์และการยืนยันตัวบุคคล (แบบฟอร์ม 1) Download!
แบบฟอร์มสมัครเป็นสมาชิกระบบเครือข่าย LDD Network (แบบฟอร์ม 2-Email address) Download!
กฎหมายที่เกี่ยวข้องโดยตรง


กฎหมายที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ
Information Technology Law
พระราชบัญญัติเผยแพร่ข้อมูลข่าวสาร พ.ศ.2540
พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2544 แก้ไขเพิ่มเติม
พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551
ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544
พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ.2550
ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานของรัฐ พ.ศ.2553
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติใน การคุ้มครองข้อมูลส่วนบุคคล ของหน่วยงานของรัฐ พ.ศ. 2553
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553
คู่มือ หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปข้อมูลอิเล็กทรอนิกส์

องค์ประกอบของนโยบาย

- ส่วนที่ 1 แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable use Policy)
- ส่วนที่ 2 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)
- ส่วนที่ 3 แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Policy)
- ส่วนที่ 4 แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail Policy)

องค์ประกอบของนโยบาย

- ส่วนที่ 5 แนวปฏิบัติการใช้งานอินเตอร์เน็ต (Internet Policy)
- ส่วนที่ 6 แนวปฏิบัติการควบคุมการเข้าถึง (Access Control Policy)
- ส่วนที่ 7 แนวปฏิบัติการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก(IDS & IPS)
- ส่วนที่ 8 การกำหนดผู้รับผิดชอบ

ส่วนที่ 1 : Acceptable use Policy

ส่วนที่ 1 : Acceptable use Policy

❖ ให้มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยมีรายละเอียด ดังนี้

1. การใช้งานบริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
2. กำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้
3. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

ส่วนที่ 1 : Acceptable use Policy

4. การแบ่งแยกเครือข่าย (Segregation in Networks) ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
5. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง
6. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ส่วนที่ 1 : Acceptable use Policy

❖ หน่วยงานมีระบบสารสนเทศในการจัดทำระบบสำรองตามแนวทาง ต่อไปนี้

1. พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
2. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

ส่วนที่ 1 : Acceptable use Policy

3. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
4. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

ส่วนที่ 1 : Acceptable use Policy

❖ หน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยมีรายละเอียด ดังนี้

1. จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
2. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วย เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ส่วนที่ 1 : Acceptable use Policy

❖ บทลงโทษและการบังคับใช้

1. กำหนดความผิด ที่เกิดขึ้นจากผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบาย ว่าด้วยความมั่นคงปลอดภัยสารสนเทศ กรมพัฒนาที่ดิน ตามเอกสาร ฉบับนี้ แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์
2. ความผิดเกี่ยวกับ นโยบายว่าด้วยความมั่นคงปลอดภัยสารสนเทศ กรมพัฒนาที่ดิน ให้ลงโทษผู้กระทำผิดตามระเบียบ กฎหมาย ที่เกี่ยวข้อง

ส่วนที่ 2 : Wireless LAN Access Control

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย Wireless LAN Access Control

ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สาย ขององค์กร จะต้องทำการลงทะเบียนกับ ผู้ดูแลระบบ และต้องได้รับอนุญาตจาก ผู้บังคับบัญชา โดยกรอกข้อมูลลงใน ***"แบบฟอร์มการขึ้นทะเบียนคอมพิวเตอร์ และการยืนยันตัวบุคคล"***

ส่วนที่ 3 : Firewall Policy

แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Policy)

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในองค์กรสามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ตได้ ในขณะที่ ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างใน ไฟร์วอลล์ได้ โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ของเครือข่าย ไฟร์วอลล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยถ้าเครือข่ายองค์กรนั้นมีการเชื่อมต่อโดยตรงกับอินเตอร์เน็ตโดยที่ไม่มีไฟร์วอลล์เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย

ส่วนที่ 4 : Use of Electronic Mail

แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมฯ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2. ผู้ใช้รายใหม่ที่ต้องการขอลงทะเบียนบัญชีชื่อผู้ใช้ ต้องทำการกรอกข้อมูล คำขอลงใน ***"แบบฟอร์มสมัครเป็นสมาชิกระบบเครือข่าย LDD Network"*** และยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน

ส่วนที่ 4 : Use of Electronic Mail

3. ผู้ใช้ไม่ควรตั้งค่าการใช้**โปรแกรมช่วยจำรหัสผ่าน**ส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

4. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมายหรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของกรมฯ

5. **ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น**เพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

ส่วนที่ 4 : Use of Electronic Mail

6. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของกรมฯ **เพื่อการทำงานของกรมฯ** เท่านั้น

7. **หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการ Logout ออกจากระบบทุกครั้ง** เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

8. ผู้ใช้ควรทำการ**ตรวจสอบเอกสารแนบ**จากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

9. ผู้ใช้**ไม่เปิดหรือส่งต่อจดหมาย**อิเล็กทรอนิกส์หรือข้อความที่ได้รับ**จากผู้ส่งที่ไม่รู้จัก**

ส่วนที่ 4 : Use of Electronic Mail

10 ผู้ใช้**ไม่ควรใช้ข้อความที่ไม่สุภาพ**หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของกรมฯ ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

11 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้**ไม่ควรระบุความสำคัญ**ของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

12 ผู้ใช้ควร**ตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน** และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

13 ผู้ใช้ควร**ลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการ**ออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 4 : Use of Electronic Mail

14 ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

15 ผู้ใช้ควรทำการสำรองข้อมูลในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอเลือกสำรองจดหมายอิเล็กทรอนิกส์ที่มีความสำคัญมาก โดยอาจทำการส่งต่อไปยังจดหมายอิเล็กทรอนิกส์แอดเดรสอื่น

16 ผู้ใช้ควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใด ๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็น และอ่านได้โดยผู้อื่น ดังนั้นการส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

ส่วนที่ 4 : Use of Electronic Mail

17 ผู้ใช้ต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัวต้องขออนุญาต ผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

18 ผู้ใช้ควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์ตอบกลับสั้น ๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้ว และจะตอบกลับอย่างสมบูรณ์ในภายหลัง

ส่วนที่ 4 : Use of Electronic Mail

19 ผู้ใช้ไม่ควรส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

20 ผู้ใช้ไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

21 ผู้ใช้ควรพิจารณาใช้ “BCC” (blind carbon copy - สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

ส่วนที่ 4 : Use of Electronic Mail

22 ผู้ใช้ควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

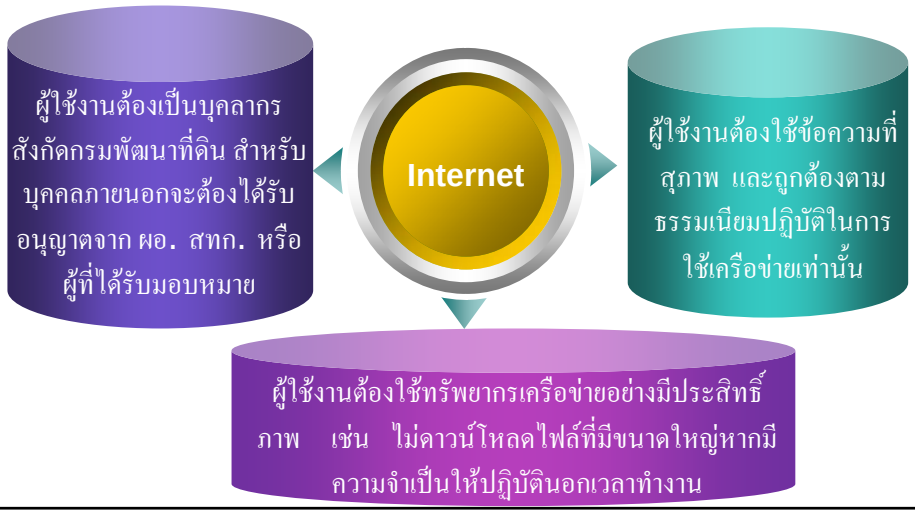
23 ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

24 จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ดังนั้นผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

25 ผู้ใช้ต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในองค์กรและสังคมถูกต้อง

ส่วนที่ 5 : Internet Policy

แนวปฏิบัติการใช้งานอินเตอร์เน็ต



ส่วนที่ 5 : Internet Policy

1. ผู้ใช้งานต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์

2. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านรหัสผู้ใช้ (User Account) ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของรหัสผู้ใช้ (User Account) ต้องเป็นผู้รับผิดชอบ

3. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

ส่วนที่ 5 : Internet Policy

4. **ผู้ใช้งานต้องไม่ใช้งาน** เพื่อการกระทำการดังต่อไปนี้
   1) เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่สถาบันชาติ ศาสนา พระมหากษัตริย์ กรมพัฒนาที่ดิน หน่วยงานอื่น และบุคคลอื่น
   2) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
   3) เพื่อการกระทำทางพาณิชย์
   4) เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน
   5) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา
   6) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว
   7) เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่ กรมพัฒนาที่ดิน

ส่วนที่ 5 : Internet Policy

4 **ผู้ใช้งานต้องไม่ใช้งาน** เพื่อการกระทำการดังต่อไปนี้

8) เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของกรมพัฒนาที่ดิน หรือของผู้ใช้อื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของกรมพัฒนาที่ดินไม่สามารถใช้งานได้ตามปกติ

9) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของกรมพัฒนาที่ดินไปยังที่อยู่ของเว็บ (website) ใด ๆ ในลักษณะที่ก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

10) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายของกรมพัฒนาที่ดิน

5 ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวทางการใช้ระบบเครือข่ายที่ กรมฯ กำหนดอย่างเคร่งครัด

ส่วนที่ 6 : Access Control Policy

1. การควบคุมเข้าออกห้อง Server

ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone)

การกำหนดสิทธิ์บุคคลในการเข้า-ออกห้อง Server โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการติดประกาศ ***"ระเบียบการเข้าออกห้อง Server"*** พร้อมระบุรายชื่อเจ้าหน้าที่ที่ได้รับการกำหนดสิทธิ์ไว้อย่างชัดเจน

กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้า-ออกห้อง Server ต้องมีมาตรการการควบคุมอย่างรัดกุม

ส่วนที่ 6 : Access Control Policy

2. การควบคุมเข้าระบบเทคโนโลยีสารสนเทศ

ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้

เจ้าของข้อมูล และเจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น

ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 6 : Access Control Policy

3. การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้

การลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

- กำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ
- กำหนดให้ผู้ใช้ลงนามในเอกสารยอมรับเงื่อนไขที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตน ใน ***"แบบฟอร์มสมัครเป็นสมาชิกระบบเครือข่าย LDD Network"***
- การกำหนดชื่อผู้ใช้ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน

ส่วนที่ 6 : Access Control Policy

4. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

1. ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

2. ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

3. ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

ส่วนที่ 6 : Access Control Policy

4. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

4. ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ

5. ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

ส่วนที่ 6 : Access Control Policy

5. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

การเข้าสู่ระบบสารสนเทศขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน อย่างน้อย 1 วิธี

การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้าหัส เป็นต้น

การเข้าสู่ระบบสารสนเทศขององค์กรจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

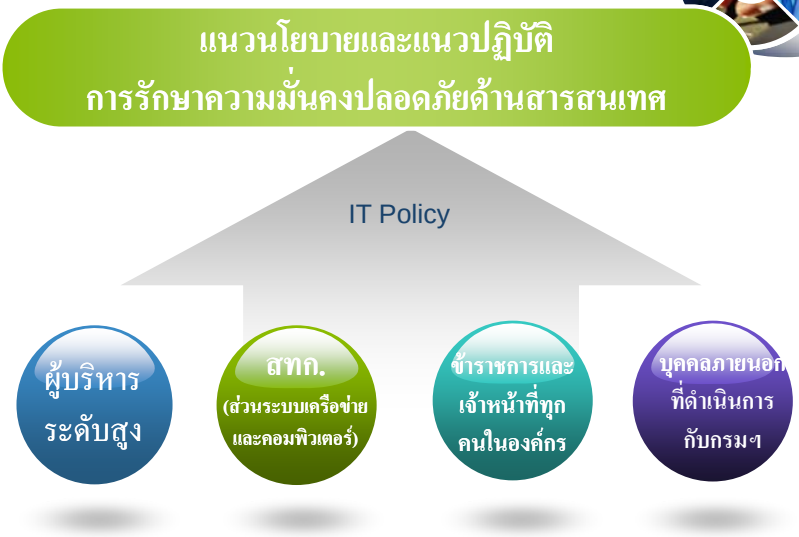
ส่วนที่ 7 : IDS & IPS

แนวปฏิบัติการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

(Intrusion Detection System: IDS and Intrusion Prevention System: IPS)

IDS (Intrusion Detection System) หรือระบบตรวจจับการบุกรุก คือ ระบบตรวจจับการบุกรุกของผู้ไม่ประสงค์ดี โดยสามารถวิเคราะห์ข้อมูลที่ผ่านเข้าออกเครือข่ายว่ามีลักษณะการทำงานที่ เป็นความเสี่ยงต่อเครือข่ายหรือไม่ โดย IDS จะทำเพียงแค่แจ้งเตือนให้ผู้ดูแลระบบทราบเท่านั้นส่วน IPS (Intrusion Prevention System) หรือระบบตรวจสอบและโต้ตอบการบุกรุกนั้น คือ ระบบที่มีลักษณะเช่นเดียวกับระบบ IDS แต่มีความสามารถมากกว่า คือ เมื่อตรวจพบข้อมูลที่มีลักษณะที่เป็นความเสี่ยงต่อเครือข่ายก็จะทำการป้องกันข้อมูลนั้นไม่ให้เข้ามาในเครือข่ายได้

ส่วนที่ 8 : การกำหนดผู้รับผิดชอบ



จบการนำเสนอ