เทคโนโลยีความปลอดภัยของข้อมูล และความเสี่ยงของการใช้ไอที

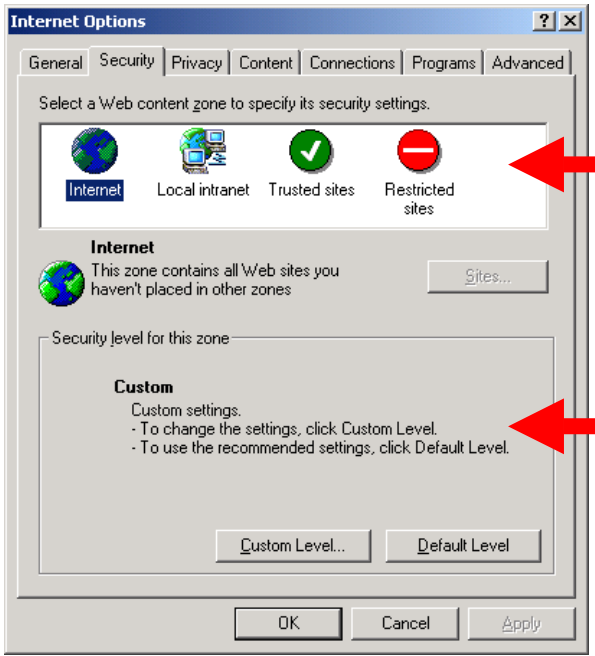
ข้อควรระวังเกี่ยวกับเว็บไซต์

- เว็บไซต์ลามกอนาจาร
  - เจาะจงเข้าไปยังเว็บไซต์ลามกอนาจาร
  - เรียกโดยอัตโนมัติจากเว็บไซต์อื่นๆ
- เว็บไซต์สปาย
  - ส่งโปรแกรมผ่านเว็บไซต์ เข้ามาเก็บข้อมูลต่างๆ ส่งกลับไปเครื่องของผู้ส่ง เช่น Cursor Comet, Data Manager
- ปัญหาการจดจำ Username และ Password ไว้ในระบบ
  - ผู้อื่นสามารถล็อกอินเข้าสู่ระบบเว็บไซต์ส่วนตัวได้

การตั้งระบบรักษาความปลอดภัยขั้นต้นด้วยตนเอง

1. เปิด IE เลือกเมนูคำสั่ง Tools, Internet Options

2. เลือกบัตรรายการ Security



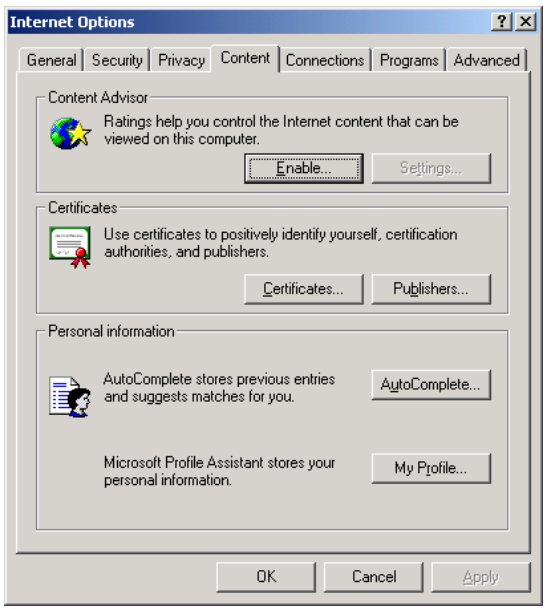
3. คลิกรูปแบบการป้องกันข้อมูล

4. คลิกเลือกระดับการรักษาความปลอดภัย

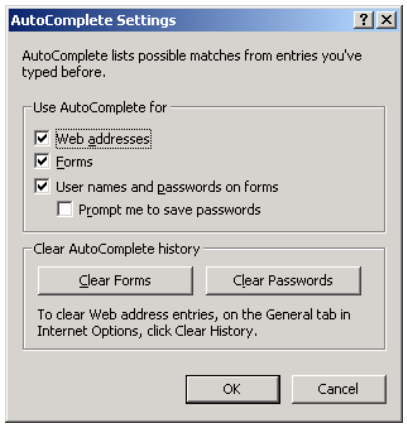
การตั้งระบบรักษาความปลอดภัยขั้นต้นด้วยตนเอง

1. เปิด IE เลือกเมนูคำสั่ง Tools, Internet Options

2. เลือกบัตรรายการ Content



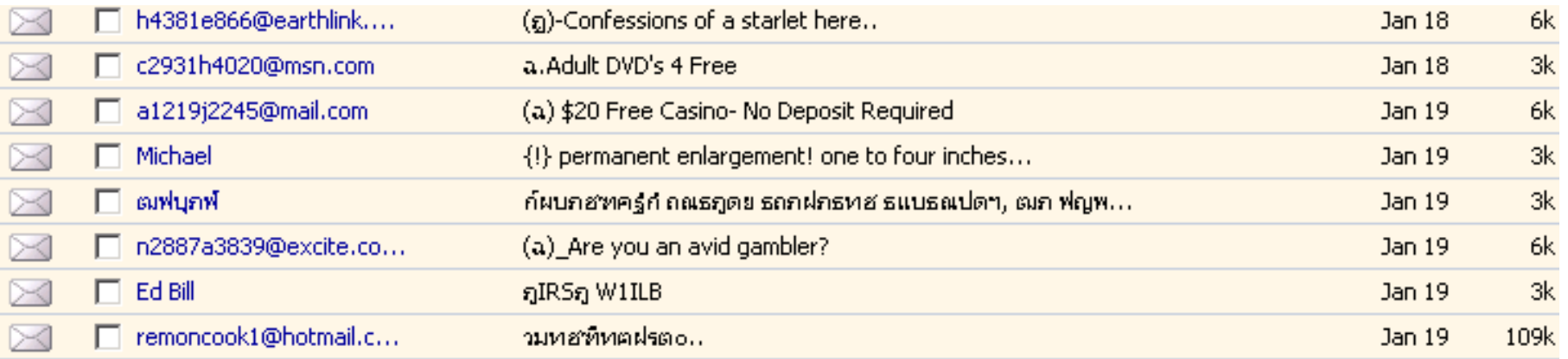
3. คลิกปุ่ม AutoComplete…



4. ยกเลิกการจำ Username & Passwor

ข้อควรระวังเกี่ยวกับอีเมล์

- อีเมล์ขยะ (Spam/Bomb Mail)
- ปัญหาไวรัส
- การล้นของ (Mailbox)
- การใช้อีเมล์โดยผู้ไม่มีสิทธิ์
- การใช้อีเมล์สำนักงาน และส่วนตัว
- การระบุข้อมูลส่วนตัวขณะขอฟรีอีเมล์

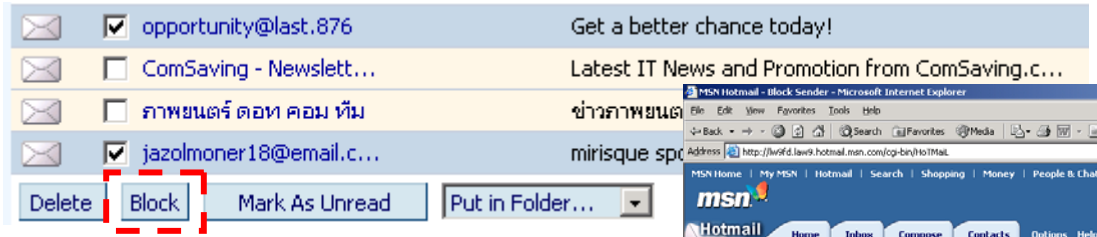


h4381e866@earthlink....	(ฐ)-Confessions of a starlet here..	Jan 18	6k
c2931h4020@msn.com	ฉ.Adult DVD's 4 Free	Jan 18	3k
a1219j2245@mail.com	(ฉ) $20 Free Casino- No Deposit Required	Jan 19	6k
Michael	{!} permanent enlargement! one to four inches...	Jan 19	3k
ฒฟนุภฟ	ก์ผบภฮฑคฐู์ก์ ถณธฦดย ธถภฝภธฑฮ ธแบธณปดฯ, ฒมภ ฟญพ...	Jan 19	3k
n2887a3839@excite.co...	(ฉ)_Are you an avid gambler?	Jan 19	6k
Ed Bill	ฦIRSฦ W1ILB	Jan 19	3k
remoncook1@hotmail.c...	วมฑฮ์ฑฑตฝรต๐..	Jan 19	109k

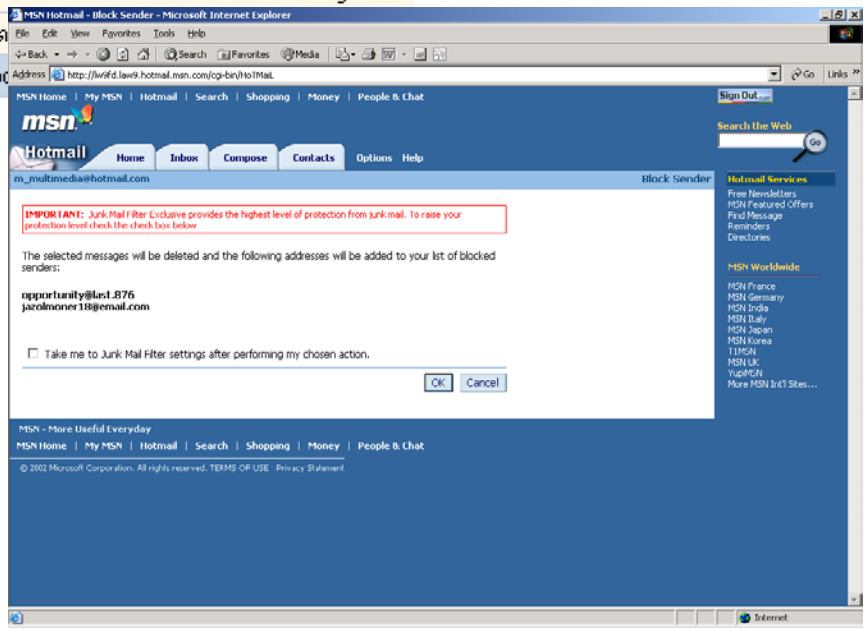
การป้องกันอีเมล์ขยะ
กรณีตัวอย่างของ Hotmail

1. เปิดเว็บไซต์ Hotmail

2. คลิกเลือกอีเมล์ที่ไม่ต้องการจาก Inbox แล้วคลิกปุ่ม Block



3. คลิก OK เพื่อยอมรับการป้องกัน

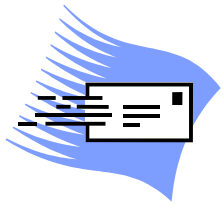


ลักษณะของธุรกรรมทางอิเล็กทรอนิกส์

- การรับส่งข้อมูลทำได้ด้วยความสะดวกรวดเร็ว
- สามารถติดตั้งระบบให้ทำการรับส่งข้อมูลแบบอัตโนมัติได้ ไร้ข้อจำกัดทางเวลาและพรมแดน
- ลดปริมาณการใช้งานกระดาษ
- การแก้ไขข้อมูลอิเล็กทรอนิกส์เป็นไปได้โดยง่าย
- การลอบดูข้อมูลอิเล็กทรอนิกส์เป็นไปได้โดยง่าย

ตัวอย่างรูปแบบการสื่อสารผ่านเครือข่ายคอมพิวเตอร์

ซื้อสินค้า 100 ชิ้น
สมศรี



ซื้อสินค้า 100 ชิ้น
สมศรี

Modem

Internet

Modem

ผู้ส่ง

ผู้รับ

การลักลอบดูข้อมูลอิเล็กทรอนิกส์

ซื้อสินค้า 100 ชิ้น
สมศรี

ซื้อสินค้า 100 ชิ้น
สมศรี

Modem

Internet

Modem

ผู้ส่ง

ซื้อสินค้า 100 ชิ้น
สมศรี

ผู้ลักลอบดูข้อมูลฯ

ผู้รับ

การลอบแก้ไขข้อมูลอิเล็กทรอนิกส์

ซื้อสินค้า 100 ชิ้น
สมศรี

ซื้อสินค้า 500 ชิ้น
สมใจ

Modem

Internet

Modem

ผู้ส่ง

ซื้อสินค้า 500 ชิ้น
สมใจ

ผู้ลักลอบแก้ไขข้อมูลฯ

ผู้รับ

ตัวอย่างการใช้ E-mail address ในการติดต่อสื่อสาร

Who am I ?

John.Smith@hotmail.com

Mayumi@yahoo.com

Somlak@thaimail.com

ไม่สามารถระบุตัวบุคคลที่แท้จริงได้

ความมั่นใจในการทำธุรกรรมอิเล็กทรอนิกส์

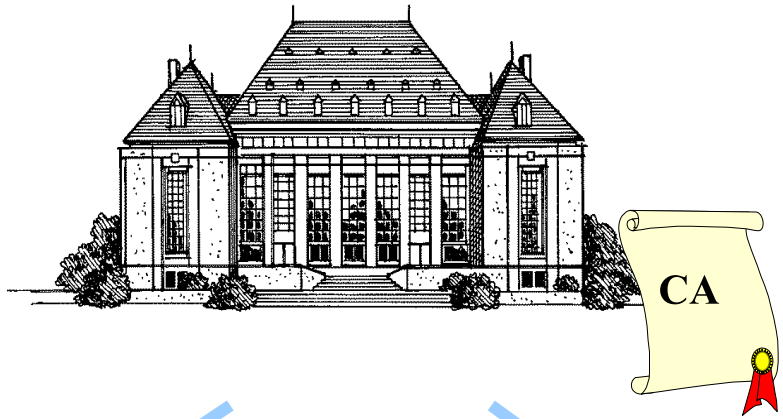
การรักษาความลับ
(Confidentiality)

ความครบถ้วนของข้อมูล
(Integrity)

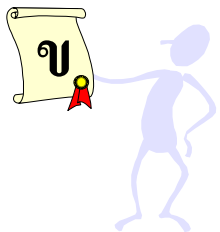
การระบุตัวบุคคล
(Authentication)

การห้ามปฏิเสธความรับผิด
(Non-repudiation)

ผู้ให้บริการออกใบรับรอง (CA)



นาย ก



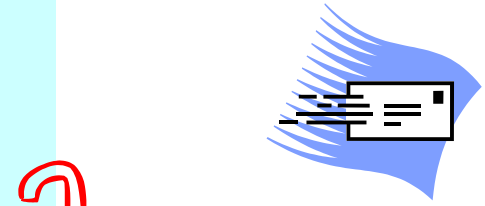
นาย ข

การใช้ใบรับรองอิเล็กทรอนิกส์กับระบบจดหมายอิเล็กทรอนิกส์

- การเข้าและถอดรหัสลับจดหมายอิเล็กทรอนิกส์
- การลงลายมือชื่อดิจิทัลกำกับจดหมายอิเล็กทรอนิกส์

การเข้าและถอดรหัสลับจดหมายอิเล็กทรอนิกส์

ดฟรกฟ หกฟ กร
รยมบ



ซื้อสินค้า 100 ชิ้น
สมศรี

Modem

Internet

Modem

ผู้ส่ง

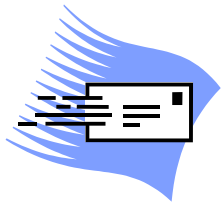
ดฟรกฟ หกฟ กร
รยมบ

ผู้รับ

ผู้ลักลอบดูข้อมูลฯ

การลงลายมือชื่อดิจิทัลกำกับจดหมายอิเล็กทรอนิกส์

ซื้อสินค้า 100 ชิ้น
สมศรี
Digital Signature



ซื้อสินค้า 100 ชิ้น
สมศรี
Digital Signature

Modem

Internet

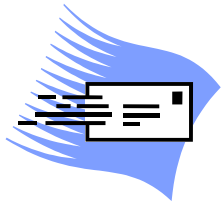
Modem

ผู้ส่ง

ผู้รับ

การลอบแก้ไขข้อมูลอิเล็กทรอนิกส์

ซื้อสินค้า 100 ชิ้น
สมศรี
Digital Signature



~~ซื้อสินค้า 500 ชิ้น~~
~~สมใจ~~
~~Digital Signature~~

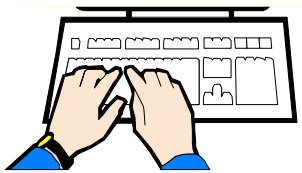
Modem

Internet

Modem

ผู้ส่ง

ซื้อสินค้า 500 ชิ้น
สมใจ
Digital Signature



ผู้ลักลอบแก้ไขข้อมูลฯ

ผู้รับ

บริการใบรับรองอิเล็กทรอนิกส์ของ สบทร.

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.)

- ผู้ให้บริการออกใบรับรองภาครัฐ

  (Government Certification Authority : G-CA)

บริการใบรับรองอิเล็กทรอนิกส์

- บริการใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล

  (Personal Certificate Service)

ประโยชน์จากการใช้งานใบรับรองอิเล็กทรอนิกส์

- ความมั่นใจในการทำธุรกรรมอิเล็กทรอนิกส์
- ความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ที่ส่งผ่านเครือข่ายอินเทอร์เน็ต
- หมดปัญหาเรื่องการปลอมแปลงหรือลักลอบแก้ไขข้อมูลอิเล็กทรอนิกส์
- ทราบถึงตัวตนที่แท้จริงของผู้ส่งข้อมูลอิเล็กทรอนิกส์

ความเสี่ยงของการใช้ไอที

- ความเสี่ยงทางกายภาพ
  - คอมพิวเตอร์หาย, เสียหายเพราะเหตุต่างๆ
- ความเสี่ยงเกี่ยวกับบุคคล
  - บุคคลที่ไม่มีสิทธิ์, บุคคลที่บุกรุกเข้ามา
- ความเสี่ยงเกี่ยวกับซอฟต์แวร์
  - ต้นฉบับของซอฟต์แวร์, ลิขสิทธิ์ต่างๆ, ไวรัสคอมพิวเตอร์
- ความเสี่ยงเกี่ยวกับระบบเครือข่าย
  - Hacker, Cracker
- ความเสี่ยงเกี่ยวกับข้อมูล
  - ระบบสำรองข้อมูล, ระบบค้นคืนข้อมูล, ระบบเข้ารหัสและถอดรหัสข้อมูล

การป้องกันความเสี่ยงด้านไอที

- ปลัดกระทรวงประกาศนโยบายการรักษาความปลอดภัยอย่างชัดเจน
- ปลัดกระทรวงแต่งตั้งผู้รับผิดชอบด้านการรักษาความปลอดภัยชัดเจน
- เจ้าหน้าที่ที่รับผิดชอบวิเคราะห์ภัยความเสี่ยงต่างๆ ที่อาจจะเกิดขึ้นได้
- เจ้าหน้าที่ที่รับผิดชอบเสนอแผนและวางมาตรการป้องกันความเสี่ยง

ตารางกำหนดระดับความเสี่ยง

ความสูญเสีย (มูลค่า บาท)	ระดับ	ความถี่
0	0	ไม่เกิด
1 - 10	1	นานๆ เกิดเหตุการณ์
11 - 100	2	ปีละครั้ง
101 - 1,000	3	ปีละหลายครั้ง
1,001 - 10,000	4	เดือนละครั้ง
10,001 - 100,000	5	เดือนละหลายครั้ง
100,001 – 1,000,000	6	วันละครั้ง
> 1,000,000	7	วันละหลายครั้ง

เหตุการณ์

เหตุการณ์	รหัส	ระดับ
ข้อมูลสูญหาย	D1	7
ข้อมูลถูกแก้ไข	D2	6
ข้อมูลเปิดใช้งานไม่ได้	D3	5
วัสดุ/อุปกรณ์สูญหาย 1 ชุด	C1	5
วัสดุ/อุปกรณ์เสียหาย 1 ชุด	C2	4
วัสดุ/อุปกรณ์เสียหายจำนวนมาก	C3	6

สถานการณ์

สถานการณ์	รหัส	ระดับ
PC ถูกใช้งานโดยไม่ได้รับอนุญาต	P1	5
PC ถูกไวรัส	P2	4
ผู้ใช้ไม่เปลี่ยนรหัสผ่าน	U1	4
มีพนักงานระบบถูกให้ออก	U2	3
Server ถูกใช้งานโดยไม่ได้รับอนุญาต	S1	4
Server ถูกไวรัส	S2	5
Server ถูก Hack	S3	7

ความเสี่ยงที่เกิดขึ้น

เหตุการณ์	สถานการณ์	ความเสี่ยง	ความหมาย
D1	S3	7/7	ข้อมูลหายเพราะ Server ถูก Hack วันละหลายครั้ง
D1	P2	7/4	ข้อมูลหายเพราะ PC ถูกไวรัส เดือนละหลายครั้ง
D2	U1	6/4	ข้อมูลถูกแก้ไขเพราะผู้ใช้ไม่เปลี่ยนรหัสทุกเดือน

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- หน่วยงานต่างๆ ควรออกข้อปฏิบัติของการใช้ไอที (Code of Conduct) เพื่อเป็นกฎระเบียบและมาตรฐานของหน่วยงาน
- ข้อปฏิบัติของการใช้ไอที ครอบคลุมทั้ง
  - ผู้บริหาร
  - เจ้าหน้าที่ดูแลระบบ
  - เจ้าหน้าที่ใช้งานทั่วไป / เจ้าหน้าที่สำนักงาน

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- ข้อปฏิบัติการกำหนดสิทธิของผู้ที่มีอำนาจในการตอบไปรษณีย์อิเล็กทรอนิกส์
- ข้อปฏิบัติเกี่ยวกับการจัดเก็บเอกสารอิเล็กทรอนิกส์
- ข้อปฏิบัติเกี่ยวกับการใช้งานระบบเครือข่าย
- ข้อปฏิบัติเกี่ยวกับการป้องกันไวรัส
- ข้อปฏิบัติเกี่ยวกับระบบรักษาความปลอดภัย

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- ข้อกำหนดเกี่ยวกับการใช้คอมพิวเตอร์
  - เจ้าหน้าที่ทุกคนต้องรับผิดชอบดูแลคอมพิวเตอร์ และอุปกรณ์ต่างๆ ของหน่วยงาน ให้อยู่ในสภาพที่พร้อมใช้งาน และมั่นรักษาความสะอาดของอุปกรณ์
  - คอมพิวเตอร์ และอุปกรณ์ต่างๆ ของสำนักงาน ไม่อนุญาตนำออกนอกหน่วยงาน โดยไม่ได้รับอนุญาต และจะต้องใช้งานเพื่องานของหน่วยงาน
  - หากคอมพิวเตอร์ หรืออุปกรณ์ใด ของหน่วยงานเกิดปัญหาข้อผิดพลาด เสีย หรือสูญหายต้องรีบแจ้งผู้บริหาร/ผู้ดูแลที่ได้รับมอบหมายหน้าที่โดยด่วน
  - ข้อมูลต่างๆ ของหน่วยงาน ทั้งในรูปของ Hard Copy และอิเล็กทรอนิกส์ให้ถือว่าเป็นข้อมูลของหน่วยงาน ไม่อนุญาตให้นำออกไปเผยแพร่โดยมิได้รับอนุญาต และให้ถือว่าทุกคนมีหน้าที่ต้องดูแลรักษาสภาพของข้อมูลให้อยู่ในรูปแบบที่เหมาะสม พร้อมใช้งาน

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- ข้อกำหนดเกี่ยวกับการใช้คอมพิวเตอร์
  - ข้อมูลในรูปแบบอิเล็กทรอนิกส์ จะต้องมีระบบสำรองข้อมูลที่เหมาะสม โดยแบ่งเป็นการสำรองข้อมูลเฉพาะบุคคล และการสำรองข้อมูลหลักของหน่วยงาน ดังนี้
    - การสำรองข้อมูลเฉพาะบุคคล ให้เจ้าหน้าที่ทุกคน ถือเป็นข้อปฏิบัติอย่างเคร่งครัด ในการสำรองข้อมูลในความรับผิดชอบของตนเอง
    - การสำรองข้อมูลหลักของหน่วยงาน ให้อยู่ภายใต้ความดูแลของ..... โดยจะต้องทำการสำรองข้อมูลจากเจ้าหน้าที่อื่นๆ ไว้ในฮาร์ดดิสก์สำรอง และแผ่นบันทึก CD-R ทุกสัปดาห์
  - การสำรองข้อมูลของหน่วยงาน จะปฏิบัติทุกวันสุดท้ายของสัปดาห์นั้น เวลา 15.00 น. ของทุกสัปดาห์ ขอให้เจ้าหน้าที่ทุกคนที่ต้องการสำรองข้อมูลกรุณานำข้อมูลทั้งหมดที่ต้องการสำรองเก็บไว้ใน C:\(ชื่อเครื่อง)_Backup เช่น D:\01_Backup และให้ Share ข้อมูลไว้เพื่อทำการสำรองข้อมูลต่อไป

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- ข้อกำหนดเกี่ยวกับระบบป้องกันไวรัส
  - เจ้าหน้าที่ทุกคน จะต้องตระหนักถึงปัญหาเกี่ยวกับไวรัส และต้องรับผิดชอบร่วมกันในการป้องกันไวรัส หากมีข้อสงสัยใดๆ ให้สอบถามผู้รับผิดชอบโดยตรง คือ .....
  - คอมพิวเตอร์ทุกเครื่อง จะต้องติดตั้งโปรแกรมป้องกันไวรัส พร้อมทำการปรับปรุงรุ่นของโปรแกรมอย่างสม่ำเสมอ ภายใต้การดูแลของ.....
  - เจ้าหน้าที่ทุกคน ต้องมั่นสำรองข้อมูลตามข้อกำหนดที่กล่าวไว้แล้ว

ข้อปฏิบัติของการใช้ไอทีในองค์กร

- **ข้อกำหนดเกี่ยวกับการสร้างเอกสารงานพิมพ์**
  - เจ้าหน้าที่ทุกคน ต้องศึกษาระบบการสร้างเอกสารงานพิมพ์ ที่ถูกต้อง และได้มาตรฐานตามกระบวนการสร้างเอกสารงานพิมพ์
  - เจ้าหน้าที่ทุกคน จะต้องช่วยกันศึกษาพัฒนาต้นแบบเอกสารงานพิมพ์ของหน่วยงานที่ถูกต้อง และได้มาตรฐาน
  - เอกสารงานพิมพ์ทุกฉบับ จะต้องยึดรูปแบบมาตรฐานของหน่วยงานดังนี้
    - ใช้ฟอนต์ AngsanaUPC
    - ขนาดตัวอักษรปกติ 16 pt.
  - มีการกำหนดหัวกระดาษ และท้ายกระดาษที่ได้มาตรฐาน
  - มีข้อความกำกับแสดงลิขสิทธิ์ของหน่วยงานในหน้ากระดาษทุกหน้า สำหรับเอกสารที่ต้องเผยแพร่ออกสู่สาธารณะ
  - ใช้หลักการตั้งชื่อไฟล์ ตามข้อกำหนดที่กล่าวมาแล้ว
  - การใช้เครื่องหมายวรรคตอนต่างๆ จะต้องเป็นไปตามระเบียบการใช้ของราชบัณฑิตยสถาน
  - การเก็บไฟล์งานเอกสารงานพิมพ์จะต้องกำหนดโฟลเดอร์เฉพาะ

ข้อปฏิบัติเกี่ยวกับการรักษาความปลอดภัยด้านไอที

- **แนวทางการป้องกันความปลอดภัยทางกายภาพของระบบ**
  - แบ่งแยกพื้นที่ควบคุมความปลอดภัยอย่างชัดเจน เช่น การแยกห้องที่เก็บเครื่องเซิร์ฟเวอร์และอนุญาตให้เฉพาะผู้ดูแลระบบเท่านั้นที่เข้าถึงได้
  - ใช้ระบบป้องกันและตรวจสอบการเข้าออกพื้นที่ควบคุมความปลอดภัย เช่น การใช้ key card ที่สามารถบันทึกได้ว่าใครเข้าออกได้ หรือการใช้กล้องวิดีโอ เป็นต้น
  - เก็บรักษาระบบและอุปกรณ์ต่างๆ เช่น backup tape, เซิร์ฟเวอร์ ในพื้นที่ควบคุมความปลอดภัย และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น
  - ใช้เครื่องจ่ายกำลังไฟฟ้าสำรองหรือ UPS เพื่อให้ระบบสามารถใช้ไฟฟ้าได้อย่างต่อเนื่อง
  - วางแผนสำหรับการกู้ระบบคืนเมื่อมีเหตุการณ์เลวร้ายเกิดขึ้น
  - ตรวจสอบข้อมูลของเจ้าหน้าที่จากภายนอกที่เข้ามาให้คำปรึกษาหรือปฏิบัติงานภายในพื้นที่ควบคุมความปลอดภัย ถ้าหากเจ้าหน้าที่ผู้นั้นต้องการใช้สิทธิของ root ในการทำงานกับระบบ ผู้ดูแลระบบจะต้องทำการ login ให้ด้วยตนเอง หลังจากนั้นต้องคอยติดตามดูว่าผู้นั้นทำอะไรกับระบบบ้าง และเมื่อเสร็จภารกิจแล้วให้ทำการเปลี่ยนรหัสผ่านของ root ทันที

ข้อปฏิบัติเกี่ยวกับการรักษาความปลอดภัยด้านไอที

- **แนวทางการป้องกันความปลอดภัยทางกายภาพภายในเครื่องคอมพิวเตอร์**
  - การล็อคเครื่องคอมพิวเตอร์ (Computer Lock) เช่น การใช้กุญแจล็อคที่ตัวเครื่อง เพื่อช่วยในการป้องกันเครื่องและอุปกรณ์ภายในเครื่องจากการถูกลักขโมย หรือทำการเปิดเครื่องเพื่อสร้างความเสียหายต่อฮาร์ดแวร์ภายในได้ และเป็นการป้องกันการรีบูตเครื่องด้วยแผ่นดิสก์หรือฮาร์ดแวร์อื่นๆด้วย
  - การรักษาความปลอดภัยใน BIOS (BIOS Security) เนื่องจาก BIOS มีความสำคัญต่อโปรแกรมที่ใช้บูตเข้าระบบ เช่น LILO ดังนั้นจึงควรปรับแต่งค่าใน BIOS เพื่อป้องกันผู้โจมตีทำการรีบูตเครื่อง มีวิธีการ โดยสรุปดังนี้
  - ปรับแต่งให้ป้อนรหัสผ่านตอนที่บูตเครื่อง ซึ่งอาจจะไม่สามารถป้องกันได้ 100% เนื่องจากผู้โจมตีสามารถทำการรีเซ็ตที่ BIOS ได้ แต่ก็เป็นการชะลอเวลาของผู้โจมตี
  - ปรับแต่งให้เครื่องไม่สามารถใช้แผ่นดิสก์ในการบูตเครื่อง
  - ปรับแต่งให้ป้อนรหัสผ่านทุกครั้งก่อนที่จะทำการปรับแต่ง BIOS
  - **หมายเหตุ**
    การตั้งรหัสผ่านตอนบูตมีข้อเสียคือ ถ้าเกิดเหตุขัดข้องบางประการ เช่น ไฟฟ้าดับเป็นเวลานาน ส่งผลให้ต้องมีการบูตใหม่ ผู้ดูแลระบบเองจะต้องอยู่ใกล้เครื่องเพื่อที่จะป้อนรหัสผ่าน มิฉะนั้นระบบจะไม่สามารถทำงานต่อไปได้

ตัวอย่างระเบียบว่าด้วยการใช้งาน ระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย

ด้วย(หน่วยงาน / บริษัท / ห้าง / ร้าน).....ได้จัดให้มีเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง เห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

"องค์กร" หมายความว่า ชื่อ (หน่วยงาน / บริษัท / ห้าง / ร้าน).....

"เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ขององค์กร.....

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร / บริษัท / ห้าง / ร้าน....

http://www.thaicert.nectec.or.th/paper/basic/policy.php