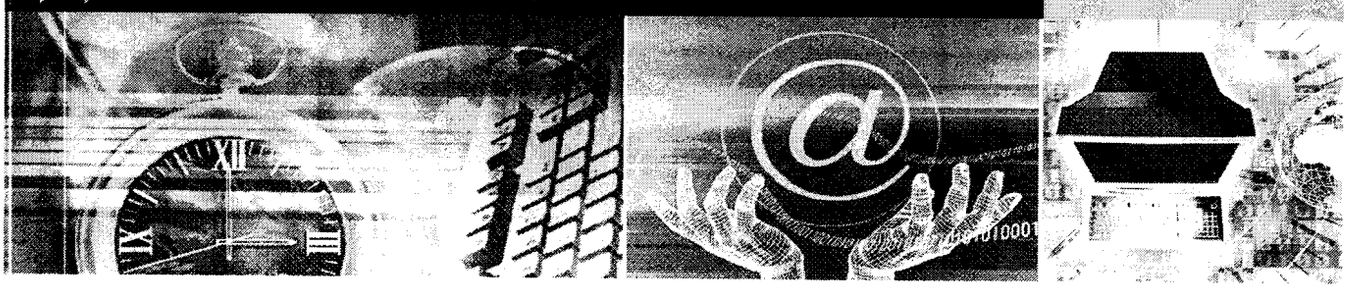
การประชุมนำเสนอร่างแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และร่างนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม

18 กุมภาพันธ์ 2553



สำนักส่งเสริมและบริการวิชาการพระจอมเกล้าลาดกระบัง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

หัวข้อการนำเสนอ

1. ร่างแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
2. ตัวอย่างร่างนโยบายความมั่นคงปลอดภัยด้าน ICT
3. ถาม - ตอบ

แนวทางการบริหารจัดการ
ความมั่นคงปลอดภัยสารสนเทศ
สำนักงานปลัดกระทรวงยุติธรรม

สำนักส่งเสริมและบริการวิชาการพระจอมเกล้าลาดกระบัง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ขอบเขตการบริหารจัดการความมั่นคง ปลอดภัยสารสนเทศ

"การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
สำหรับการบริการเทคโนโลยีสารสนเทศและการสื่อสาร
ของสำนักงานปลัดกระทรวงยุติธรรม"

บริการ ICT ได้แก่

- ศูนย์คอมพิวเตอร์
- ระบบเครือข่ายคอมพิวเตอร์
- ระบบสารสนเทศกลาง

ร่างนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ -1

วัตถุประสงค์

วัตถุประสงค์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำนักงานปลัดกระทรวงยุติธรรม เพื่อให้มั่นใจว่าการปฏิบัติงานตามภารกิจหลักและสนับสนุน ตลอดจนการบริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานปลัดกระทรวงยุติธรรม จะเป็นไปอย่างต่อเนื่องและมีเสถียรภาพ ตลอดจนมีความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ข้อมูลและทรัพย์สินที่เกี่ยวข้องในการดำเนินงานจากภัยคุกคามอยู่ในระดับที่ยอมรับได้ โดยการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะประยุกต์ใช้กรอบแนวทางปฏิบัติของมาตรฐาน ISO 27001:2005

ร่างนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ -2

นโยบาย

- เป้าหมายของนโยบายเพื่อป้องกันทรัพย์สินสารสนเทศ (Information Assets) ของสำนักปลัดกระทรวงยุติธรรมจากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือเป็นอุบัติเหตุก็ตาม
- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต้องอนุมัตินโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ และให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้ระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง

ร่างนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ -3

นโยบาย (ต่อ)

❖ นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องการสร้างความมั่นใจดังนี้

- สารสนเทศจะต้องถูกป้องกันจากผู้ไม่มีสิทธิในการเข้าถึง (unauthorized access)
- สารสนเทศจะต้องถูกรักษาสถานภาพด้านความลับ (Confidentiality)
- สารสนเทศจะต้องถูกรักษาสถานภาพด้านความถูกต้องสมบูรณ์ (Integrity)
- สารสนเทศจะต้องมีสถานภาพพร้อมใช้งาน (Availability) ตามความต้องการทางธุรกิจ
- การปฏิบัติตามคำสั่ง ระเบียบ ข้อบังคับ กฎหมาย และข้อตกลง ที่มีผลต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ
- แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติจะต้องถูกพัฒนา ปรับปรุง และทดสอบ
- บุคลากรของสำนักงานปลัดกระทรวงยุติธรรม จะต้องได้รับการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
- ทุก ๆ เหตุการณ์ที่เกิดขึ้นที่มีผลต่อกระทบต่อการรักษาความมั่นคงปลอดภัยสารสนเทศจะต้องถูกบันทึก ตรวจสอบ จัดการและรายงาน
- นโยบาย ขั้นตอน และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ต่าง ๆ จะต้องถูกกำหนดเพื่อสนับสนุนนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการตรวจสอบ การประเมิน และมีการปรับปรุงอย่างต่อเนื่องให้เหมาะสมกับสถานการณ์ที่เปลี่ยนไป

7

ร่างนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ -4

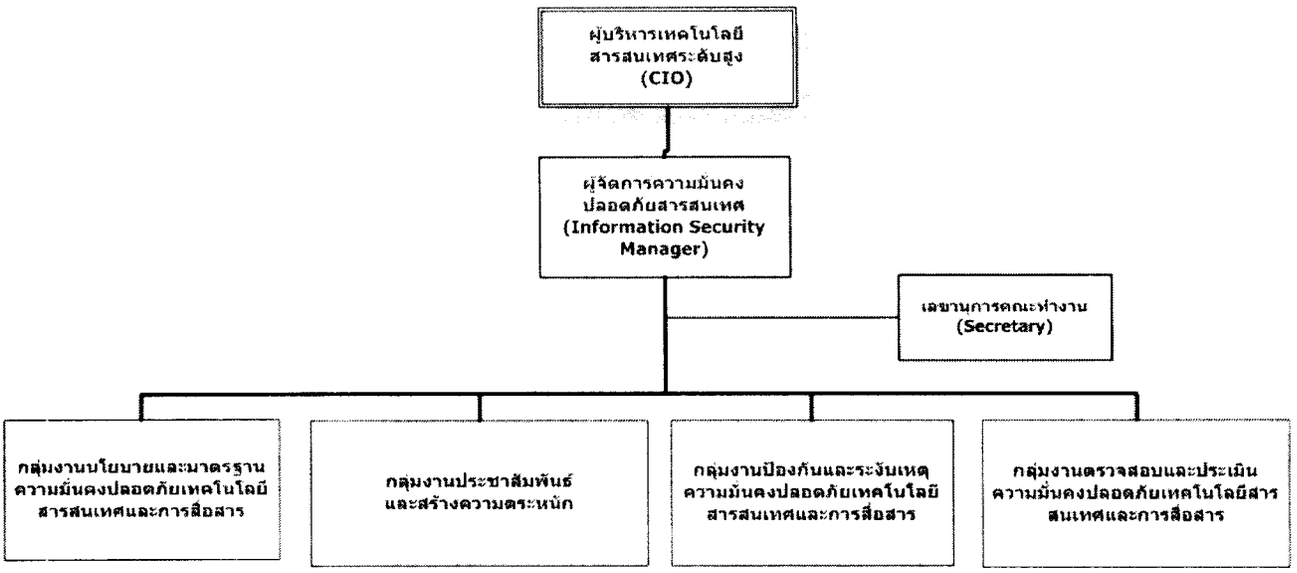
นโยบาย (ต่อ)

❖ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

❖ ต้องมีการแต่งตั้งผู้จัดการความมั่นคงปลอดภัยสารสนเทศ และคณะทำงานเป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานปลัดกระทรวงยุติธรรม

❖ นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจะต้องถูกนำไปปฏิบัติอย่างเคร่งครัด

ร่างโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ



ตัวอย่างร่างนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงยุติธรรม

สำนักส่งเสริมและบริการวิชาการพระจอมเกล้าลาดกระบัง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

3.1 การจัดทำบัญชีสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ขององค์กรได้รับการป้องกันและปกป้องอย่างเหมาะสม

<u>นโยบาย</u>

3.1.1 ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

1) ต้องจัดทำและเก็บบัญชีรายการสินทรัพย์ ซึ่งรวมถึง สินทรัพย์ข้อมูลและเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อสินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ขององค์กร โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานการจัดการสินทรัพย์สารสนเทศขององค์กร

2) ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง หรือภายใน 1 เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เป็นต้น

3) ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของสินทรัพย์ เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

3.1.2 ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

1) ต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบ ข้อมูลและสินทรัพย์ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สป. กระทรวงยุติธรรมอย่างชัดเจน

3.1.3 การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

1) จะต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและสินทรัพย์จะต้องถูกใช้ โดยต้องปฏิบัติตามข้อกำหนดในเอกสารคู่มือการปฏิบัติงานการจัดการสินทรัพย์สารสนเทศขององค์กร

3.1 การจัดทำบัญชีสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ขององค์กรได้รับการป้องกันและปกป้องอย่างเหมาะสม

2) การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานขององค์กร การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
- เจ้าหน้าที่ ตลอดจนบุคคล และ/หรือนิติบุคลที่ได้รับว่าจ้างโดยสำนักงาน จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของสำนักงาน
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ขององค์กร อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งหมดขององค์กร ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายขององค์กร รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ขององค์กร ก่อนได้รับอนุญาต
- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในองค์กร อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงานการรักษาความปลอดภัยสารสนเทศสำหรับการเดินทาง (Information Security for Guideline for Traveling)
- อุปกรณ์คอมพิวเตอร์ขององค์กร ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และเจ้าหน้าที่ ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ขององค์กร อย่างเด็ดขาด

3.1 การจัดทำบัญชีสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ขององค์กรได้รับการป้องกันและปกป้องอย่างเหมาะสม

3) การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ขององค์กร
- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญขององค์กร ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศขององค์กร
- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปขององค์กร มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้อำนวยการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานขององค์กรเท่านั้น

3.1 การจัดทำบัญชีสินทรัพย์ (Responsibility for Assets)

วัตถุประสงค์: เพื่อให้สินทรัพย์ขององค์กรได้รับการป้องกันและปกป้องอย่างเหมาะสม

4) การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

- องค์กรจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัยการค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการขององค์กร
- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้องค์กร และบุคคลผู้ที่เกี่ยวข้องกับองค์กร เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ องค์กร ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- องค์กรไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

3.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม

นโยบาย

3.2.1 วิธีการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines)

1) เจ้าหน้าที่ต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
2) เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลดิจิตอลหรือสารสนเทศดิจิตอลนั้น

3.2.2 การจัดทำป้ายชื่อ และการจัดการข้อมูลสารสนเทศ (Information Labeling and Handing)

1) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูล และอุปกรณ์สินทรัพย์สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร
2) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

3.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม

3) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น
4) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม
5) ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน
6) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ โดยทันที
7) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล
8) เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับขององค์กรในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหาร ฯลฯ
9) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, Thumb-Drive, CD-Rom เป็นต้น) ที่มีข้อมูลลับขององค์กร บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง
10) ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานขององค์กรทั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งาน ต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใด ๆ เกิดขึ้น ตัวอย่างเช่น การติดไวรัส ฮาร์ดดิสก์เสีย เป็นต้น