บทที่ 3

ขั้นตอนการได้มาของกุญแจรหัสส่วนตัว

จากการใช้สภาพแวดล้อมของจุฬาลงกรณ์มหาวิทยาลัยเป็นกรณีศึกษาของวิทยานิพนธ์ ผู้ทำวิจัยได้ทำการสัมภาษณ์อย่างไม่เป็นทางการกับเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ และการสอบถามเจ้าหน้าที่ ภาควิชาวิศวกรรมคอมพิวเตอร์ ของจุฬาลงกรณ์มหาวิทยาลัย ในเรื่องของโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure – KPI) พบว่า

1) ปัจจุบันมหาวิทยาลัยยังไม่มีการนำกุญแจคู่สาธารณะมาใช้งาน แต่คาดว่ามีการเตรียมการที่จะนำมาใช้ในอนาคตเนื่องจากความเป็นมหาวิทยาลัยของรัฐ และรัฐบาลมีนโยบายในการประยุกต์ใช้งานเทคโนโลยีดังกล่าวกับหน่วยงานของรัฐ

2) ระบบคอมพิวเตอร์ของมหาวิทยาลัยเป็นลักษณะของสภาพแวดล้อมแบบปิด ซึ่งส่วนมากฝ่ายต่างๆที่เกี่ยวข้องจะรู้จักกันและมักมีความสัมพันธ์ในเชิงสัญญากันอยู่แล้วการติดต่อระหว่างบุคคลต่างๆในองค์กรเดียวกันผ่านเครือข่ายอินทราเน็ตซึ่งในบางกรณีบุคคลที่สองและสามอาจเป็นบุคคลเดียวกันทำให้เหลือฝ่ายต่างๆที่เกี่ยวข้องเพียงสองฝ่าย (two-party model)

3) ผู้ใช้งานหรือผู้ที่มีส่วนเกี่ยวข้องสามารถแยกได้ออกสองส่วนคือ เจ้าหน้าที่ระดับทั่วไปซึ่งยังไม่มีความรู้ในเทคโนโลยีกุญแจรหัสคู่สาธารณะ และ คณะอาจารย์และผู้บริหารของมหาวิทยาลัยที่ยังไม่มีความเชื่อถือในด้านความปลอดภัยของการใช้งานดังกล่าว

4) บุคลากรระดับต่างๆ รวมถึงผู้บริหารยังไม่เห็นความสำคัญและขาดแรงจูงใจในการที่จะนำเทคโนโลยีของกุญแจรหัสส่วนตัวมาใช้งาน ตลอดจนการปกป้องดูแลรักษาเพื่อไม่ให้สูญหายหรือถูกล่วงรู้ โดยบุคคลอื่น ซึ่งอาจเกิดขึ้นได้จากกรณีที่มีการนำกุญแจรหัสส่วนตัวของบุคคลอื่นไปใช้งาน เช่น การไหว้วานหรือมอบหมายในการทำธุรกรรมแทน โดยเจ้าของกุญแจรหัสส่วนตัวเป็นผู้อนุญาตให้บุคคลอื่นเข้าใช้แทนตน

5) ในมหาวิทยาลัยมีสำนักเทคโนโลยีสารสนเทศ เป็นหน่วยงานหลักที่คอยให้บริการด้านสารสนเทศแก่หน่วยงานหรือภาควิชาต่างๆของมหาวิทยาลัย ในสำนักเทคโนโลยีสารสนเทศประกอบด้วยส่วนหลักๆ 3 ส่วนคือ 1. ธุรการ 2. สารสนเทศ และ 3. เครือข่าย และมีการดำเนินงานในด้านการรักษาความปลอดภัยอย่างเป็นระบบ ผู้วิจัยเห็นว่าสำนักเทคโนโลยีสารสนเทศมีความพร้อมและเหมาะสมเป็นหน่วยงานหลักในการนำเสนอการนำเทคโนโลยีกุญแจ

คู่สาธารณะมาใช้งานในจุฬาต่ออธิการบดีโดยผ่านตามลำดับขั้นเช่น หัวหน้าฝ่าย ผ่าน ผอ.ฝ่าย ผ่าน รองอธิการบดีฝ่ายบริหารกายภาพ เพื่อเสนอเรื่องถึง อธิการบดี

จากสภาพแวดล้อมดังกล่าวจึงนำมาตรฐานด้านความปลอดภัยมาปรับให้เหมาะสมเพื่อสร้างขั้นตอนการปฏิบัติงานที่เชื่อถือได้เพื่อการได้มา และการใช้งานระยะยาวของกุญแจรหัสส่วนตัว โดยการนำมาตรฐาน ISO/IEC17799, CobiT, ITIL และ HIPPAA ซึ่งมาตรฐานที่นิยมในการนำมาเป็นแนวทางในการเตรียมระบบสารสนเทศขององค์กร [5] ซึ่งมาตรฐานแต่ละมาตรฐานนั้นไม่สามารถนำมาแทนที่ซึ่งกันและกันได้แต่ละมาตรฐานจะมีวัตถุประสงค์หลักต่างกัน

มาตรฐาน CobiT นั้นมีพื้นฐานมาจาก Framework ชั้นนำต่างๆมากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO 9000 และของ ITIL (The Information Technology Infrastructure Library) ด้วย มาตรฐาน CobiT เป็น Framework ที่เน้นในเรื่องของ การควบคุม (Control) เป็นหลักนั้นก็ยังขาดในส่วนต่างๆดังต่อไปนี้ คือประเด็นในการบอกว่าองค์กรต้องการอะไรบ้าง (What) แต่ไม่มีรายละเอียดในแง่ของวิธีการที่นำไปสู่จุดนั้น (How) ซึ่งเหมาะกับผู้ตรวจสอบระบบสารสนเทศที่ต้องการนำ CobiT มาใช้เพื่อทำเป็น Check Lists หรือ Audit Program แต่อาจจะยังไม่มีรายละเอียดพอสำหรับ ผู้บริหารซึ่งต้องการนำ CobiT ไปปรับใช้กับองค์กรในทางปฏิบัติ (Practical Implementation)

มาตรฐาน ITIL นั้น มีวัตถุประสงค์ในการสร้าง "Best Practices" สำหรับกระบวนการของ IT Service Delivery และ Support แต่ไม่ได้เป็นการกำหนด Framework ของการควบคุมในแนวกว้างอย่างที่ CobiT เป็น ITIL นั้นจะมุ่งไปทางการเสนอวิธีการในการปฏิบัติ แต่มีขอบเขตงานเพียงแค่ IT service Management ซึ่งแคบกว่า CobiT มาก ITIL นั้นค่อนข้างลึกในรายละเอียดของกระบวนการทำงาน ซึ่งมีวัตถุประสงค์ที่จะให้ทางฝ่ายระบบสารสนเทศ และ Service Management เป็นผู้นำไปใช้

ISO/IEC 17799 มีจุประสงค์หลักในด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ (Information Security) เน้นการตรวจสอบด้านกระบวนการและการควบคุมด้านความปลอดภัย (Improve security processes and controls) ในมาตรฐานของ ISO จะบอกถึงขั้นตอนในการที่ต้องทำแต่ไม่บอกว่าแต่ละขั้นตอนที่ต้องทำนั้นมีรายละเอียดว่าต้องทำอย่างไรเหมือนกันกับมาตรฐานของ CobiT ตารางที่ 3.1 จะแสดงในส่วนประกอบของการนำมาตรฐานดังกล่าวมาเปรียบเทียบในส่วนการทำงานของตน

จากแนวทางการอ้างอิงจากมาตรฐานต่างๆสามารถทำการเทียบเคียงและเสริมขั้นตอนการทำงานซึ่งทำให้ได้กรอบแนวทางในนโยบายด้านต่างๆกระบวนการ และรูปแบบวิธีปฏิบัติออกเป็นขั้นตอนโดยแบ่งออกเป็น 5 ข้อหลัก และนำเสนอขั้นตอนที่น้อยที่สุดที่ควรจะต้องมีในการปฏิบัติ ตลอดจนไปถึงการเสนอแนวทางเพื่อให้ผู้บริหารยอมรับเพื่อการนำไปใช้งานซึ่งมี

รายละเอียดดังตารางที่ 3.2 ขั้นตอนการปฏิบัติงานเพื่อการได้มาและรักษากุญแจรหัสส่วนตัวและแสดงการนำมาตรฐานที่อ้างอิงในการนำมาใช้ในขั้นตอนการปฏิบัติงานดังกล่าวที่ภาคผนวก ก.

ITIL	COBIT	ISO/IEC 17799
แนวคิด/กระบวนการ (Concept/Process)	ปัจจัยสำคัญของความสำเร็จ (Critical Success Factors)	ความปลอดภัยของข้อมูล (Information Security)
กิจกรรม Activities	มาตรฐานตัวชี้วัด Metrics (CSF, KPi)	
การคุ้มค่าการลงทุน Cost/Benefit	การเทียบเคียงสมรรถนะ Benchmarking (CMM)	
การวางแผนในการนำไปใช้ Planning for implementation	การควบคุม Controls	
	การตรวจสอบ Audit	

ตารางที่ 3.1 การแสดงองค์ประกอบของมาตรฐานเพื่อการเปรียบเทียบ [6]

ขั้นตอนการปฏิบัติงานเพื่อการได้มาและรักษากุญแจรหัสส่วนตัว	
ลำดับที่	**ขั้นตอนปฏิบัติงาน**
1.0	นโยบายด้านความปลอดภัย (Security Policy)
2.0	การเตรียมการด้านความปลอดภัย (Preparation)
	2.1 สถานที่ตั้งในการทำงานขององค์กรและใช้สร้างกุญแจรหัสส่วนตัว
	2.2 การควบคุมการเข้าถึง หรือใช้งานอุปกรณ์ต่างๆทางกายภาพ
	2.3 การเตรียมการป้องกันภัยธรรมชาติ
	2.4 การเตรียมการเก็บสื่อบันทึกข้อมูลและการทำลาย
	2.5 ด้านบุคลากร
3.0	รูปแบบใบรับรองอิเล็กทรอนิกส์และกุญแจรหัสส่วนตัว
	3.1 หน้าที่ของผู้ออกใบรับรองอิเล็กทรอนิกส์
	3.2 หน้าที่ของบุคลากรที่เกี่ยวข้องกับความปลอดภัย
	3.3 การสร้างกุญแจรหัสส่วนตัว
	3.3.1 การสร้างกุญแจรหัสของพนักงานปฏิบัติการ
	3.3.2 การสร้างกุญแจรหัสของผู้บริหาร
4.0	แนวทางการป้องกันกุญแจรหัสส่วนตัว

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	4.1 วิธีการกำหนดแนวทางการป้องกันหรือตรวจสอบความปลอดภัยในการที่จะใช้งานกุญแจ	
	4.2 แนวทางการป้องกันกุญแจรหัสส่วนตัวสำหรับผู้บริหาร	
5.0	การตรวจสอบประเมินความเสี่ยงด้านการใช้งาน	
ข้อปฏิบัติที่น้อยที่สุดที่ควรมีในด้านความปลอดภัย		
	1.0 นโยบายด้านความปลอดภัย (Security Policy)	
	จุดประสงค์ : เพื่อเป็นแนวทางให้ผู้บริหารกำหนดทิศทางและนโยบายต่างในการดำเนินการใช้กุญแจรหัสลับในองค์กร และเป็นผู้ให้การสนับสนุนช่วยเหลือการปฏิบัติงาน	
1.1	ผู้บริหารต้องแสดงเจตจำนงในการนำระบบการใช้งานกุญแจรหัสส่วนตัวเข้ามาใช้งานในองค์กร	ผู้บริหาร
1.2	ผู้บริหารองค์กร ต้องเห็นชอบและรับรู้ในการที่จะกำหนดบทบาทหน้าที่ความรับผิดชอบและความสัมพันธ์ต่อกัน ทั้งได้สร้างการสื่อสารให้ทราบกันภายในองค์กร ตลอดจนต้องมีส่วนร่วมในการรับผิดชอบภายใต้บทบาทและหน้าที่ที่ได้กำหนดไว้	ผู้บริหาร
1.3	ผู้บริหารองค์กรต้องสนับสนุนกิจกรรมในการดำเนินงานและส่งเสริมเพื่อให้ระบบสามารถดำเนินการลุล่วงทั้งในด้าน บุคลากรและการเงิน โดยอยู่ภายใต้แผนงานที่ได้กำหนด	ผู้บริหาร
1.4	รับรองการจัดตั้งคณะทำงานในด้านความปลอดภัยของกุญแจรหัสลับ ผู้บริหารองค์กร ต้องจัดตั้งคณะกรรม หรือกลุ่มผู้ทำงานหลักเพื่อบริหารและจัดการความมั่นคงปลอดภัยทั้งหมดขององค์กร	ผู้บริหาร

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
1.5	จัดทำ เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร และนโยบายนี้จะต้องได้รับอนุมัติจากผู้บริหารสูงสุดขององค์กรในการที่นำไปใช้	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
1.6	อนุญาตให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยให้พนักงานทุกระดับในองค์ที่ต้องมีส่วนเกี่ยวข้องทราบ	ผู้บริหาร
1.7	จัดทำบัญชีทรัพย์สินที่มีทั้งหมดในองค์กร โดยการบันทึกจัดทำเป็นบัญชีทรัพย์สินขององค์กรทั้งหมดที่มีอยู่ทั้งหมดภายในองค์กร และต้องมีการตรวจสอบทุกๆช่วงเวลาที่กำหนดเช่นทุก 6 เดือนจะต้องมีการตรวจสอบทรัพย์สินว่ายังอยู่ครบถ้วน สมบรูณ์และพร้อมใช้งาน	เจ้าหน้าที่ปฏิบัติงาน
1.8	มีการตรวจสอบติดตามทรัพย์สินต่างๆที่มีในองค์ได้ ว่าอยู่ที่ใดสถานะเป็นอย่างไร และมีข้อมูลรายละเอียดต่างๆของทรัพย์สินนั้นเช่น วัน/เดือน/ปีที่ซื้อ การรับประกัน ประวัติการซ่อมบำรุง ผู้ดูแลรับผิดชอบ	เจ้าหน้าที่ปฏิบัติงาน
1.9	การดูแลรักษาความปลอดภัยทรัพย์สินต่างๆ ต้องจัดให้มีมาตรการรักษาความปลอดภัยให้กับห้องทำงานตลอดจนเครื่องมืออุปกรณ์ต่างๆเช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญต้องไม่สามารถเข้าถึงได้ง่ายๆจากบุคคลอื่น หรือไม่ติดตั้งตามทางผ่านของบุคลากรทั่วไป	เจ้าหน้าที่ปฏิบัติงาน
1.10	จัดสรรพื้นที่การรับผิดชอบความปลอดภัยให้สามารถดูแลด้านความปลอดภัยได้อย่างทั่วถึง	เจ้าหน้าที่ปฏิบัติงาน
1.11	เตรียมพื้นที่ในการส่งมอบวัสดุหรือผลิตภัณฑ์ต่างๆ โดยจัดแยกเป็นพื้นที่ในการส่งมอบแยกออกจากพื้นที่ควบคุมสำคัญโดยมีมาตรการ การตรวจสอบวัสดุหรือผลิตภัณฑ์ ผู้จัดส่ง เอกสารเกี่ยวข้องต่างๆเช่นใบขนส่งของที่ถูกต้องและป้องกันจากผู้ไม่มีส่วนเกี่ยวข้องให้เข้ามาในส่วนรักษาความปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
1.12	การสร้างสิ่งขวางกั้นเพื่อกำหนดบริเวณความปลอดภัยต้องมีการสร้างกำแพง หรือ ผนังรอบรอบบริเวณที่จัดให้มีการสร้างกุญแจรหัสลับและห้ามติดประกาศแผนที่หรือบอกที่ตั้งห้องใดๆทั้งสิ้น	เจ้าหน้าที่ปฏิบัติงาน
1.13	การควบคุมการเข้า-ออก บริเวณองค์กรสร้างมาตรการรักษาความปลอดภัยในการควบคุมบริเวณที่จัดให้เป็นพื้นควบคุม อย่างเข้มงวด ไม่อนุญาตให้ผู้ไม่มีสิทธิเข้าออกโดยเด็ดขาด	เจ้าหน้าที่ปฏิบัติงาน
1.14	การสร้างห้องสำหรับสร้างกุญแจรหัสลับต้องมีการสร้างห้องที่ถูกออกแบบมาให้มีความเหมาะสมต่อการปฏิบัติงานในการใช้เป็นพื้นที่ ในการสร้างกุญแจรหัสลับส่วนตัว โดยต้องมีระบบความปลอดภัยสูงสุด	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
1.15	เตรียมการสำรองการใช้ไฟฟ้าให้เพียงพอในกรณีไฟฟ้าดับและมีตารางการทดสอบ	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
1.16	ทำการคงอุณหภูมิให้มีความเหมาะสมต่อการปฏิบัติงาน ทั้งความเย็นและความชื้นที่เหมาะสม	เจ้าหน้าที่ปฏิบัติงาน
1.17	วางแผนการปรับปรุงอุปกรณ์ต่างๆเพื่อให้ทันสมัยและมีประสิทธิภาพ	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	2.0 การเตรียมการด้านความปลอดภัย (Preparation)	
	จุดประสงค์ : เตรียมความพร้อมในด้านความปลอดภัยที่จำเป็นพื้นฐานต่างๆเพื่อรองรับการนำกุญแจรหัสส่วนตัวมาใช้งาน	
	2.1 สถานที่ตั้งในการทำงานขององค์กรและใช้สร้างกุญแจรหัสส่วนตัว	
2.1.1	วางแบบแปลนการจัดสรรพื้นที่ ตำแหน่งห้อง กำแพง ผนังที่มีความแข็งแรงปิดล้อมบริเวณที่ต้องการความมั่นคงปลอดภัย	ผู้บริหาร / หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
2.1.2	กำหนดจุดติดตั้งโทรทัศน์วงจรปิด เพื่อบันทึกเหตุการณ์ภายในองค์กรและในการติดตั้งนั้นต้องแน่ใจได้ว่าไม่สามารถถูกดับจับหรือขโมยสัญญาณได้	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
2.1.3	ติดตั้งระบบการป้องกันผู้บุกรุกโดยไม่ได้รับอนุญาต เช่นสามารถจับการเคลื่อนไหว	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	เช่นมีการส่งสัญญาณเมื่อมีการบุกรุกผ่านจุดที่กำหนด	
2.1.4	ควรมีการติดตั้ง เครื่องดักจับความสั่นสะเทือนหรือการถูกโจรกรรม เช่น สัญญาณเตือนภัยจะทำงานเมื่อกระจกหรือประตูถูกทำลายเป็นต้น	เจ้าหน้าที่ปฏิบัติงาน
2.1.5	การตรวจสอบการเปิด ปิดของประตูหรือหน้าต่าง ตลอดจนช่องทางในการเข้าถึงภายในที่ทำงานได้ เช่น ส่งสัญญาณเตือนเมื่อมีการเปิดค้างของประตู	เจ้าหน้าที่ปฏิบัติงาน
2.1.6	มีอุปกรณ์ตรวจจับควันที่อาจเกิดจาก อัคคีภัย หรือ สารระเหย ไวไฟ	เจ้าหน้าที่ปฏิบัติงาน
2.1.7	การป้องกันการบุกรุกจากภายใต้ห้องปฏิบัติการหรือใต้ดินควรมีเครื่องตรวจวัดความสั่นสะเทือนของพื้นดิน หรือ ติดตั้งสัญญาณป้องกันการเจาะจากใต้ดิน	เจ้าหน้าที่ปฏิบัติงาน
2.1.8	ติดตั้งสารดับเพลิงที่ไม่ทำลายอุปกรณ์สำคัญๆ เช่นคอมพิวเตอร์หรือมีการเตรียมการป้องกันอุปกรณ์สำคัญต่างๆนั้นไว้กรณีเกิดไฟไหม้	เจ้าหน้าที่ปฏิบัติงาน
	2.2 การควบคุมการเข้าถึง หรือใช้งานอุปกรณ์ต่าง ๆทางกายภาพ	
2.2.1	การเข้าหรือ ออก พื้นที่ควบคุมให้เฉพาะผู้มีสิทธิเท่านั้น และห้ามสวมหมวกใดๆ หรือผ้าคลุมหน้า ตลอดจนแว่นดำเข้ามาในบริเวณดังกล่าว	เจ้าหน้าที่ปฏิบัติงาน
2.2.2	บันทึกภาพด้านหน้าตรงของบุคคลที่เข้าออกในบริเวณรักษาความปลอดภัยหรือสถานที่สำคัญทุกครั้ง พร้อมทั้งวันเวลาในการเข้าออกนั้นด้วย	เจ้าหน้าที่ปฏิบัติงาน
2.2.3	มีการควบคุมบุคคลที่เข้าออกบริเวณควบคุมด้วย การทดสอบตั้งแต่สองชนิดขึ้นไปเช่น Biometric + Smart Cart หรือ รหัสผ่านประตู + บัตรประจำตัว + การถ่ายภาพบุคคลเข้าพื้นที่ เป็นต้น	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
2.2.4	ไม่ติดตั้งเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อทางเครือข่ายหรือคอมพิวเตอร์ส่วนบุคคลทุกชนิดที่ใช้งานสำคัญไว้ในบริเวณที่มีผู้คนเข้าออกสม่ำเสมอ	เจ้าหน้าที่ปฏิบัติงาน
2.2.5	ต้องทำการล็อคหรือใส่กุญแจประตู หน้าต่าง ทุกห้องที่ไม่มีผู้ปฏิบัติงานอยู่	เจ้าหน้าที่ปฏิบัติงาน
2.2.6	ไม่มีการอนุญาตให้มีการบันทึกต่างๆ เช่น วีดีโอ กล่องถ่ายรูปชนิดต่างๆในบริเวณพื้นที่รักษาความปลอดภัย	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.2.7	อุปกรณ์การทำสำเนาทุกชนิด เช่น เครื่องถ่ายเอกสาร สแกนเนอร์ เป็นต้น ต้องใช้เจ้าหน้าที่เป็นผู้ดำเนินการให้เท่านั้นและต้องมีการบันทึกการใช้งานตลอดจนมีการป้องกันการใช้งานจากบุคคลอื่น	เจ้าหน้าที่ปฏิบัติงาน
2.2.8	ไม่มีการขนย้ายใดๆจากในองค์กรออกสู่ภายนอกโดยไม่ได้รับอนุญาต ต้องมีเอกสารรับรองการขนย้ายหรือนำสิ่งของ คอมพิวเตอร์ อุปกรณ์ทุกชนิด ออกไปต้องมีผู้รับผิดชอบในการขนย้ายนั้นๆ	เจ้าหน้าที่ปฏิบัติงาน
2.2.9	ต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง	ผู้บริหาร /เจ้าหน้าที่ปฏิบัติงาน / ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.2.10	ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับพนักงานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.2.11	ตั้งเวลาในเครื่องคอมพิวเตอร์ให้ตรงกันและเทียบกับเวลามาตรฐานกลางของโลก	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.2.12	ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ดังนี้ 2.12.1 ต้องทำการพิสูจน์ตัวตนก่อนการใช้งาน 2.12.2 ให้ทำการโปรแกรมระบบงานแยกออกจากโปรแกรมยูทิลิตี้	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	2.12.3 การติดตั้งใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น 2.12.4 ทำการบันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้หรือโปรแกรม	
	2.3 การเตรียมการป้องกันภัยธรรมชาติ	
2.3.1	การป้องกันจากอัคคีภัย ด้วยการติดตั้งระบบดับเพลิงอัตโนมัติโดยใช้สารที่มีคุณสมบัติพิเศษในการดับเพลิงอย่างมีประสิทธิภาพ เช่น FM-200 เป็นต้น	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.3.2	การป้องกันภัยจากน้ำโดยจัดสภาพแวดล้อมให้มีการป้องกันภัยอันเกิดจากน้ำเช่น การระบายน้ำกรณีเกิดน้ำท่วมหรือการยกพื้นให้มีความสูงจากระดับพื้นปกติ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.3.4	จัดให้มีสายล่อฟ้าป้องกันกรณีฟ้าผ่าและมีการเดินสายดิน	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.4 การเตรียมการเก็บสื่อบันทึกข้อมูลและการทำลาย	
2.4.1	เตรียมการจัดเก็บสื่อบันทึกต่างๆในสถานที่ปลอดภัยและการจัดเก็บที่เป็นระบบมีผู้รับผิดชอบในการดูแลจัดเก็บ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.4.2	มีการจัดเก็บบันทึกการเข้าใช้งานระบบ เช่น ผู้ใช้รหัสผ่าน เวลาการเข้าใช้งาน ระยะเวลา มีการลบหรือทำลายข้อมูลหรือไม่ ต้นทางมากจากแอดเดรสเครื่องใด โดยเก็บข้อมูลไว้ในสื่อบันทึกเช่น ดีวีดี เป็นต้น	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
2.4.3	สื่อบันทึกข้อมูลในรูปแบบต่างๆที่ไม่ใช้ต้องถูกทำลายจนแน่ว่าไม่สามารถจะกู้คืนมาได้ เช่นการทำลายด้วยการเขียนทับซ้ำ ทำลายด้วยสนามแม่เหล็ก การบดละเอียด ใช้กรดกัดทำลาย หรือการทำไปเผาไฟ เป็นต้น	เจ้าหน้าที่ปฏิบัติงาน
	2.5 ด้านบุคลากร	
2.5.1	บุคลากรทุกคนต้องปฏิบัติตามงานภายใต้ข้อกำหนดระเบียบวิธีปฏิบัติว่าด้วยความมั่นคงของข้อมูล	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	ที่ได้กำหนดขึ้นอย่างเคร่งครัด ดังเช่น	
	2.5.1.1ทำสัญญาลงนามในการรักษาความลับที่สำคัญ และการเปิดเผยข้อมูลที่ปกปิดตลอดจนวิธีการดำเนินงานของเจ้าหน้าที่กับหน่วยงาน	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.1.2 กำหนดให้มีกฎระเบียบการลงโทษต่อการฝ่าฝืน หรือละเมิดนโยบายความมั่นคงปลอดภัยของหน่วยงาน	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.1.3 รายงานให้ผู้ที่รับผิดชอบทราบทันทีที่พบสิ่งผิดปกติทั้งในส่วนที่เป็นซอฟต์แวร์หรือ การทำงานของอุปกรณ์ต่างๆ	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.1.4 ห้ามนำอุปกรณ์ไปใช้ผิดประเภทหรือ ไปใช้นอกขอบเขตของการหน้าที่อุปกรณ์นั้นๆ	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.1.5 ตรวจสอบหรือทำบันทึกการทำงานและประวัติการทำงาน การซ่อมบำรุง ของอุปกรณ์ต่างๆ ในส่วนที่ตนรับผิดชอบ	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.1.6 เครื่องมือหรืออุปกรณ์ต่างๆ เจ้าหน้าที่ไม่สามารถนำเข้ามาปฏิบัติได้ ให้ใช้เครื่องมือหรืออุปกรณ์ทุกชนิดตามที่ได้ผ่านการตรวจสอบมาแล้วเท่านั้น	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
2.5.2	การสรรหา	
	2.5.2.1 วัดความรู้ความสามารถในส่วนที่ต้องรับผิดชอบของงานที่ต้องเข้ามาปฏิบัติ	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ/ เจ้าหน้าที่ปฏิบัติงาน
	2.5.2.2 ทดสอบทัศนคติ อารมณ์ การแก้ปัญหากรณีการทำงานรับผิดชอบภายใต้ความกดดันสูง โดยอาจทดสอบกับ แบบทดสอบทางจิตวิทยาที่เชื่อถือได้ เป็นต้น	
	2.5.2.3 ตรวจสอบประวัติของบุคลากร ประวัติอาชญากรรม ประวัติการทำงาน ตลอดจนลักษณะ	

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	พื้นฐานทางครอบครัว การศึกษา ผู้รับรอง	
	2.5.2.4 ตรวจสอบสุขภาพ เช่น โรคติดต่อที่ร้ายแรง สายตา โรคประจำตัว	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
	2.5.2.5 กำหนดหน้าที่ความรับผิดชอบของงานให้กับผู้ที่จะรับผิดชอบทราบ รวมถึงกฎระเบียบ เงื่อนไขต่างๆที่มี	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง
2.5.3	การเตรียมบุคลากรและจำนวนกำลังคนในการปฏิบัติหน้าที่ให้มีความปลอดภัยและมีประสิทธิภาพ	ผู้บริหาร
	2.5.3.1 ต้องไม่มีการรับผิดชอบในตำแหน่งที่สำคัญด้วยบุคลากรเพียงคนเดียว เช่น ตำแหน่ง เจ้าหน้าที่ดูแลระบบ ต้องมีการทำงานอย่างน้อย 2 คนที่รับผิดชอบในหน้าที่ดังกล่าวและต้องไม่มีความสัมพันธ์ที่ใกล้ชิดกัน เช่น เป็นเพื่อนหรือ ญาติพี่น้อง	ผู้ดูแลระบบ ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.2 ในการปฏิบัติงานต้องมีการจัดทำบัญชีตารางในการทำงานโดยต้องสามารถตรวจสอบได้ว่า เจ้าที่ใดที่ปฏิบัติงานอยู่ในช่วงเวลาปัจจุบัน	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.3 เจ้าที่ปฏิบัติงานทุกคน ต้องผ่านกระบวนการตรวจสอบตัวตนของเจ้าหน้าที่นั้น และมีการบันทึกรายละเอียดการเข้าทำงานอย่างชัดเจน เช่น วันเวลาของผู้ปฏิบัติ ผู้ตรวจสอบ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.4 จัดให้มีการฝึกอบรมเทคโนโลยี หรือความรู้ใหม่ๆด้านความมั่นคงปลอดในเจ้าหน้าที่ ที่เกี่ยวข้อง เช่น การป้องกันโปรแกรมไวรัส ซอฟต์แวร์ป้องกันการโจมตีหรือการดักจับการบุกรุก	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.5 จัดประชุมทบทวนนโยบายความปลอดภัย กฎระเบียบ การปฏิบัติที่ถูกต้องและมีประสิทธิภาพ ตลอดจนแจ้งรายงาน ข้อมูลข่าวสาร ความเคลื่อนไหวให้เจ้าหน้าที่ได้รับทราบเป็นประจำ	ผู้บริหาร/ ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	2.5.3.6 ฝึกอบรมการรับมือต่อเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น การรับมือเมื่อมีการละเมิดหรือบุกรุกความมั่นคงปลอดภัย การเรียนรู้ ,ทบทวนพัฒนาการปฏิบัติงาน	ผู้บริหาร/ ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.7 การทำรายงาน การแจ้งเหตุ ตลอดจนวิธีการสังเกตสิ่งผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.8 ทดสอบความสามารถในการปฏิบัติงานของเจ้าหน้าที่เป็นประจำ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.9 ส่งเจ้าหน้าที่ไป ดูงาน ฝึกอบรม หรือ ฝึกงานกับ หน่วยงานที่มีประสิทธิภาพหรือมีความสามารถในเรื่องความปลอดภัยของ กุญแจรหัสลับ	ผู้ดูแลระบบ /เจ้าหน้าที่ปฏิบัติงาน
	2.5.3.10 การจัดทำคู่มือหรือเอกสารการปฏิบัติงานตลอดจนการใช้งานและดูแลรักษาอุปกรณ์ต่างๆในสำนักงาน	เจ้าหน้าที่ปฏิบัติงาน
	3.0 รูปแบบของใบรับรองอิเล็กทรอนิกส์และกุญแจรหัสส่วนตัว	
	จุดประสงค์: เป็นแนวทางในการกำหนดหน้าที่และการปฏิบัติของผู้ให้ใบรับรองอิเล็กทรอนิกส์และกุญแจรหัสส่วนตัว	
3.1	หน้าที่ของผู้ออกใบรับรองอิเล็กทรอนิกส์ ในการใช้งานของกุญแจรหัสส่วนตัวนั้นปัญหาสำคัญคือการไว้เชื่อมั่นหรือไว้ใจในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์กับผู้เกี่ยวข้องด้วยจึงต้องมีการรับรองผู้อ้างตนด้วย ใบรับรองอิเล็กทรอนิกส์ ซึ่งสร้างมาจากองค์กรที่น่าเชื่อถือและไว้ใจได้ ซึ่งบทบาทหน้าที่ของผู้ออกใบรับรองมีดังนี้คือ	
	3.1.1 ให้บริการและจัดการด้านเครื่องคอมพิวเตอร์สำหรับ ระบบให้บริการใบรับรองในด้านต่างๆ	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	เช่น ระบบปฏิบัติการ การกำหนดตัวแปรสำคัญ เป็นต้น	
	3.1.2 บริหารจัดการระบบจัดเก็บข้อมูลของระบบให้บริการใบรับรอง เช่นแบบฟอร์มคำร้องขออนุมัติใบรับรองการเตรียมเอกสารเพื่อขอใบรับรอง เป็นต้น	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.3 รับคำขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.4 ออกใบรับรองให้กับผู้ขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.5 รับคำขอเพิกถอนใบรับรอง	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.6 เพิกถอนใบรับรองตามคำร้องขอของผู้ใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.7 พิสูจน์ความถูกต้องและตัวตนของผู้ขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.8 การเผยแพร่ใบรับรองอิเล็กทรอนิกส์	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.9 การเรียกคืนใบรับรองอิเล็กทรอนิกส์	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.10 แจ้งข้อมูลข่าวสาร ความเคลื่อนไหว การเปลี่ยนแปลง ให้กับที่ผู้มีส่วนเกี่ยวข้องในข้อมูลที่กระทบต่อสิทธิ หน้าที่	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.11 อำนวยความสะดวกให้แต่ผู้ขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.12 มีวิธีการเก็บข้อมูลเอกสารหลักฐานในสถานที่ที่ปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.13 มีการประกาศถ้อยแถลงในแนวทางขั้นตอนการออกใบรับรอง (Certification Practice Statement)	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.14 ปรับปรุงข้อมูลของผู้ถูกรับรองให้ทันสมัย	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
3.2	การทำหน้าที่ของบุคลากรที่เกี่ยวข้องกับความปลอดภัยระดับสูงเช่น ผู้ควบคุมระบบ ควรจะปฏิบัติดังนี้	
	3.2.1 ทำบัญชีการใช้งานเจ้าหน้าที่ทุกตำแหน่ง	เจ้าหน้าที่ปฏิบัติงาน
	3.2.2 การควบคุมดูแล บริหารจัดการงานที่สำคัญต้องมีผู้รับผิดชอบในตำแหน่งดังกล่าวอย่างน้อย 2 คน เช่นตำแหน่งผู้ดูแลระบบ	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
	3.2.3 การเปลี่ยนแปลงแก้ไขกุญแจของระบบให้บริการให้เป็นปัจจุบันต้องต้องกำหนดให้มีผู้รับผิดชอบอย่างน้อย 3 คน ที่ไม่มีความสัมพันธ์ส่วนบุคคลร่วมกันรับผิดชอบ	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
	3.2.4 การทำงานต่างๆ ต้องมีหลักฐานที่สามารถสืบย้อนไปได้เช่น เวลาเข้าออกการเข้าใช้เครื่องคอมพิวเตอร์ การใช้บริการต่างๆที่มีให้บริการ เป็นต้น	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ/ เจ้าหน้าที่ปฏิบัติงาน
3.3	การสร้างกุญแจรหัสส่วนตัว มีขั้นตอนต่างๆเป็นแนวทางดังนี้คือ	
	3.3.1 การสร้างกุญแจรหัสของพนักงานปฏิบัติการ	
	3.3.1.1 แสดงหลักฐานและเอกสารคำร้องขอสร้างกุญแจรหัสส่วนตัว เช่น บัตรประจำตัวประชาชน แบบฟอร์มที่กำหนด เป็นต้น	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.2 เมื่อผ่านการตรวจสอบเอกสารที่ยื่นว่าถูกต้อง ครบถ้วน สมบรูณ์แล้วเจ้าหน้าที่จะทำการนัดเพื่อสร้างกุญแจรหัสส่วนตัว	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.3 ในการเข้าไปห้องปฏิบัติการจะมีระเบียบและข้อบังคับต่างๆให้ปฏิบัติตามในการสร้างกุญแจคู่สาธารณะ	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	3.3.1.4 ผู้สร้างรหัสต้องเป็นผู้ดำเนินการตั้งแต่ต้นจนจบ และในกรณีที่มีข้อสงสัยในการปฏิบัติจะมีวีดีโอ แนะนำที่สามารถปฏิบัติตามขั้นตอนไปพร้อมๆกันได้	เจ้าหน้าที่ปฏิบัติงาน
	3.3.1.5 ในกระบวนการสร้างกุญแจคู่สาธารณะนั้น กุญแจรหัสส่วนตัวที่สัมพันธ์กับกุญแจสาธารณะ นั้นจะต้องมอบให้ผู้สร้างทันทีหลังจากเสร็จกระบวนการโดยอาจอยู่ในรูปของ Smart Card ซึ่งอาจมีการตั้งรหัสผ่านในการที่จะ Active โดยอาจมีการใช้เทคนิคของ Token keys of key มาเสริม เป็นต้นส่วนกุญแจสาธารณะจะนำไปขอใบรับรองอิเล็กทรอนิกส์ต่อไป	เจ้าหน้าที่ปฏิบัติงาน
	3.3.2 การสร้างกุญแจรหัสของผู้บริหาร	
	3.3.2.1กำหนดหน้าที่ความรับผิดชอบในการเตรียมเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆที่ใช้ในการสร้างรหัสกุญแจส่วน โดยไม่ทำการต่อพ่วงกับเครือข่ายใดๆ และทำการตรวจสอบปลอดภัยในอุปกรณ์ต่างๆ ซึ่งกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบอย่างน้อย 2 คน	เจ้าหน้าที่ปฏิบัติงาน
	3.3.2.2 ต้องมีการควบคุมการเข้าออกในบริเวณที่จัดไว้ให้ผู้บริหารซึ่งอาจเป็นห้องทำงานผู้บริหารเองไม่ให้การ เข้า-ออก ขณะทำการสร้างรหัส	เจ้าหน้าที่ปฏิบัติงาน
	3.3.2.3 ผู้บริหารต้องเป็นผู้ดำเนินการในการสร้างกุญแจรหัสในเครื่องคอมพิวเตอร์และอุปกรณ์ที่เตรียมไว้ตั้งแต่ต้นจนจบ กรณีที่มีข้อสงสัยในการปฏิบัติจะมี วีดีโอ ที่เจ้าหน้าที่ได้เตรียมไว้แล้วคอยแนะนำให้ผู้บริหารสามารถปฏิบัติตามขั้นตอนไปพร้อมๆกันได้	เจ้าหน้าที่ปฏิบัติงาน
	3.3.2.4 ในกระบวนการสร้างกุญแจคู่สาธารณะนั้น กุญแจรหัสส่วนตัวที่สัมพันธ์กับกุญแจ	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	สาธารณะ นั้นจะต้องมอบให้ผู้บริหารทันทีหลังจากเสร็จกระบวนการโดยอาจอยู่ในรูปของ Smart Card ซึ่งอาจมีการตั้งรหัสผ่านในการที่จะ Active โดยอาจมีการใช้เทคนิคของ Token keys of key มาเสริม	
	3.3.2.5 กุญแจสาธารณะของผู้บริหาร จะนำไปขอใบรับรองอิเล็กทรอนิกส์โดยอยู่ภายใต้การรับรู้และความเข้าใจของผู้บริหาร	เจ้าหน้าที่ปฏิบัติงาน
3.4	ขั้นตอนการขอใบรับรอง มีอยู่ด้วยกัน 2 ประเภทคือ	
	3.4.1 ใบรับรองเครื่องแม่ข่ายซึ่งมีขั้นตอนพอสังเขปดังนี้	
	3.4.1.1 ส่งกุญแจสาธารณะ ชื่อที่แตกต่าง (Distinguished name) และชื่อทั่วไป (Common name) ให้แก่องค์กรที่จะใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	3.4.1.2 กรอกแบบฟอร์มข้อมูลและ เอกสารต่างๆที่ผู้ให้บริการร้องขอ	เจ้าหน้าที่ปฏิบัติงาน
	3.4.1.3 การส่งต้องแน่ใจว่ามีความปลอดภัย โดยอาจเข้ารหัสด้วยกุญแจสาธารณะขององค์กรที่ต้องการขอใบรับรอง เป็นต้น	เจ้าหน้าที่ปฏิบัติงาน
	3.4.1.4 เมื่อเอกสารต่างๆผ่านการพิจารณาแล้ว องค์กรที่รับรองออกใบรับรองให้ จะประกอบด้วยกุญแจสาธารณะของผู้ขอและข้อมูลอื่นๆที่เกี่ยวข้อง โดยองค์กรนั้นจะรับรองโดยการลงลายมือชื่ออิเล็กทรอนิกส์ กับความถูกต้องส่งมาด้วย	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	3.4.2 ใบรับรองบุคคลหรือเครื่องลูกข่าย	
	3.4.2.1 กรอกแบบฟอร์มข้อมูลที่องค์กรต้องการพร้อมทั้งจัดส่งข้อมูลที่ร้องขอเช่น บัตรประจำตัวประชาชน จัดส่งด้วยช่องทางที่ปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน
	3.4.2.2 รอการตรวจสอบเอกสารและการยืนยัน	เจ้าหน้าที่ปฏิบัติงาน
	3.4.2.3 ทำสัญญากับองค์กรรับรอง	เจ้าหน้าที่ปฏิบัติงาน
	3.4.2.4 นำไปใช้งานตามเงื่อนไขที่ทางองค์กรรับรองแจ้งให้ทราบ	เจ้าหน้าที่ปฏิบัติงาน
	4.0 แนวทางการป้องกันกุญแจรหัสส่วนตัว	
	จุดประสงค์: เพื่อแนวทางในการใช้งานและป้องกันกุญแจรหัสส่วนตัวทั้งนักปฏิบัติการทั่วไปและผู้บริหาร	
4.1	วิธีการกำหนดแนวทางการป้องกันหรือตรวจสอบความปลอดภัยในการที่จะใช้งานกุญแจรหัสส่วนตัวซึ่งมีแนวทางดังนี้	
	4.1.1 การกำหนดมาตรฐานขั้นต่ำ (Baseline) โดยเปรียบเทียบกับมาตรฐานการรักษาความปลอดภัยเช่น Department of Defense Computer System Center (DoDCSC) หรือของ Trust Computer System Evaluation Criteria (TCSEC) เป็นการวัดระดับการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ที่ได้ใช้งานอยู่ (Measurement of Trust) ซึ่งได้จัดไว้เป็น 3 กลุ่มเรียงจากความน่าเชื่อถือน้อยไปมากได้ดังนี้	หัวหน้างานระบบสารสนเทศ
	4.1.1.1 ระดับความน่าเชื่อถือ D Minimum Security เป็นความปลอดภัยพื้นฐานของระบบที่ต้องมี	
	4.1.1.2 ระดับความน่าเชื่อถือ C Discretionary Protection การรักษาความปลอดภัยเป็นส่วนๆที่จำเป็น	

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	4.1.1.3 ระดับความน่าเชื่อถือ B Mandatory Protection การรักษาความปลอดภัยทั้งระบบตามมาตรฐานที่ได้กำหนดไว้ 4.1.1.4 ระดับความน่าเชื่อถือ A Verified Protectionการรักษาความปลอดภัยของระบบในขั้นสูงสุด	หัวหน้างานระบบสารสนเทศ
	4.1.2 ทำการตรวจสอบระบบ เพื่อประทำการประเมินความเสี่ยงของช่องโหว่ต่างๆของระบบ (Vulnerability Assessment)	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	4.1.3 ตรวจสอบระบบ (Audit) ตลอดจนอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยทั้งด้านฮาร์ดแวร์และซอฟแวร์	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	4.1.4 เก็บข้อมูลที่ได้จากการตรวจสอบ (Inventory) ให้เป็นระบบ	เจ้าหน้าที่ปฏิบัติงาน
	4.1.5 ทำการประเมินความเสี่ยงจากข้อมูลที่ได้จากการทดสอบแล้วจัดลำดับความเสี่ยงที่สูงที่สุดเพื่อจะได้แก้ไขก่อน	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
	4.1.6 ทำการปิดความเสี่ยงภัยที่ประเมินได้ เช่นการปรับเปลี่ยนรหัส ไปจนถึงการทำ Hardening ระบบโดยอาจมีการปรับเปลี่ยนแก้ไขค่าติดตั้งของระบบ	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	4.1.7นำระบบหรือเทคโนโลยีด้านความปลอดภัยมาเสริมสนับสนุนตรวนสอบเช่น IPS (Intrusion Prevention System) หรือ (Scan and Block Technology)	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
	4.1.8 ปรับปรุง Patch หรือนำระบบ Patch Management System มาใช้งานตลอดจนทำการปรับเปลี่ยนขั้นตอนการทำงาน (Workflow)	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	4.1.9 ทำการตรวจสอบติดตามด้านความปลอดภัยตามขั้นตอนที่กล่าวมาอยู่เสมอ และปฏิบัติหรือติดตามความเปลี่ยนแปลงของเทคโนโลยีด้านความปลอดภัยอยู่เสมอ	เจ้าหน้าที่ปฏิบัติงาน
	4.1.10 ล็อคเครื่องคอมพิวเตอร์ที่สำคัญ (Computer Lock) เช่นการใช้กุญแจล็อคที่ตัวเครื่องเมื่อไม่ใช้งาน	เจ้าหน้าที่ปฏิบัติงาน
	4.1.11 ติดตั้งรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนตัวเช่นปรับแต่งโปรแกรม Boot Loader ของLinux	ผู้ดูแลระบบ
	4.1.12 ล็อคหน้าจอคอมพิวเตอร์ (Screen Lock) ทุกครั้งเมื่อพักการใช้งาน	เจ้าหน้าที่ปฏิบัติงาน
	4.1.13 ล็อคไฟล์ต่างๆที่มีลักษณะดังนี้คือ 4.1.13.1 ล็อคไฟล์ที่ไม่สมบรูณ์หรือขาดหายไป 4.1.13.2 ล็อคไฟล์ที่มี Timestamp ผิดปกติ 4.1.13.3 ล็อคไฟล์ที่มี Permission เช่นการล็อคไฟล์ระบบที่เจ้าของเป็น user	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	4.1.14 ข้อมูลของการรีบูตเครื่องหรือการทำการรีสตาร์ท Service	ผู้ดูแลระบบ
	4.1.15 การใช้คำสั่ง su หรือการ login เข้ามาจากต้นทางที่ผิด	ผู้ดูแลระบบ
	4.1.16 ไม่มอบหมายให้ผู้อื่นผู้ใดกระทำธุรกรรมอิเล็กทรอนิกส์โดยใช้กุญแจรหัสของตน	เจ้าหน้าที่ปฏิบัติงาน
	4.1.17 ไม่นำกุญแจรหัสไปใช้งานในสภาพแวดล้อมที่ขาดความน่าเชื่อถือ เช่นการเข้าไปใช้งานในเว็บที่ไม่แน่ใจว่าปลอดภัยเป็นต้น	ผู้ใช้งานกุญแจหรัส
	4.1.18 ตรวจสอบการดูการเปลี่ยนแปลงของความปลอดภัยทาง กายภาพที่เกิดขึ้น (Detecting Physical Security Compromises) 4.1.18.1 ติดตั้งโปรแกรม ป้องกันไวรัส หนอนคอมพิวเตอร์ สปายแวร์	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	4.1.18.2 ใช้ความระมัดระวังในการโหลดหรือติดตั้งโปรแกรม โดยเฉพาะโปรแกรมที่มีที่มาหรือผู้ผลิตไม่ชัดเจนหรือไม่น่าเชื่อถือ	เจ้าหน้าที่ปฏิบัติงาน
	4.1.18.3 ไม่ทำการต่อเชื่อมเครือข่ายหรืออินเตอร์เน็ตก่อนจะติดตั้งระบบคุ้มกันภัย	เจ้าหน้าที่ปฏิบัติงาน
	4.1.18.4 ใช้โปรโตคอลที่สนับสนุนระบบรักษาความปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน
	4.1.19 ไม่เปิดการใช้งานบริการต่างๆที่ไม่สำคัญเช่น ftp, telnet, finger, rpc, mail, rservices	ผู้ดูแลระบบ
	4.1.20 ต้องมีความระมัดระวังกุญแจรหัสของตนนับตั้งแต่ได้รับการครอบครอง	ผู้ใช้งานกุญแจรหัส
	4.1.21 เมื่อมีข้อสงสัยหรือพิรุธที่สังเกตเห็น ต้องทำการแจ้งให้กับ ผู้มีส่วนเกี่ยวข้องรับผิดชอบทันที	ผู้ใช้งานกุญแจรหัส
	4.1.22 ไม่เปิดเผยข้อมูลใดๆของตนให้กับเว็บไซต์หรือบุคคลอื่นใดที่ไม่มีความมั่นใจ	ผู้ใช้งานกุญแจรหัส
	4.1.23 ตั้งรหัสผ่านในการเข้าสู่ระบบให้ยากต่อการคาดเดา	เจ้าหน้าที่ปฏิบัติงาน
	4.1.24 ทำการเปลี่ยนกุญแจรหัสใหม่ทันทีเมื่อเกิดเหตุการณ์ดังนี้ 4.1.24.1 มีการขโมยรหัสหรือทำซ้ำ 4.1.24.2 สูญหายหรือใช้การไม่ได้ 4.1.24.3 มีผู้อื่นล่วงรู้กุญแจส่วนตัว 4.1.24.4 มีการเปลี่ยนแปลงข้อมูลในใบรับรอง 4.1.24.5 มีการยกเลิกการใช้งาน 4.1.24.6 ต้องการเปลี่ยนรหัสใหม่ 4.1.24.7 มีปัญหาการถูกโจมตีหรือเจาะระบบของผู้ให้บริการออกใบรับรอง	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
4.2	การป้องกันกุญแจรหัสส่วนตัวสำหรับผู้บริหาร	
	4.2.1 ต้องมีเจ้าหน้าที่รับผิดชอบดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์ที่ใช้งานของผู้บริหาร ต้องจัดให้มีมาตรการรักษาความปลอดภัยให้กับห้องทำงานตลอดจนเครื่องมืออุปกรณ์ต่างๆของผู้บริหาร	เจ้าหน้าที่ปฏิบัติงาน
	4.2.2 การใช้งานเครื่องคอมพิวเตอร์ส่วนตัวของผู้บริหารจะทำการกรอง MAC Address ที่กำหนดค่าที่ระบุให้ใช้โดยการกำหนดตารางที่อนุญาตและไม่อนุญาต ตลอดจนติดตั้งระบบความปลอดภัยในเครื่องผู้บริหารด้วย	เจ้าหน้าที่ปฏิบัติงาน
	4.2.3 ติดตั้งระบบการป้องกันผู้บุกรุกโดยไม่ได้รับอนุญาต เช่นสัญญาณเตือนภัย	เจ้าหน้าที่ปฏิบัติงาน
	4.2.4 มีการมีการควบคุมการเข้าออกห้องผู้บริหาร การทดสอบตั้งแต่สองชนิดขึ้นไปเช่น Biometric + Smart Cart หรือ รหัสผ่านประตู + บัตรประจำตัว + กุญแจประตู	เจ้าหน้าที่ปฏิบัติงาน
	4.2.5 ต้องล็อคหรือใส่กุญแจทุกห้องทำงานที่ผู้บริหารไม่อยู่	เจ้าหน้าที่ปฏิบัติงาน
	4.2.6 ผู้บริหารต้องไม่นำกุญแจรหัสส่วนตัวไปใช้งานในสถานที่ที่ไม่แน่ใจถึงความปลอดภัยเช่น เว็บไซต์ทั่วไป	ผู้บริหาร
	4.2.7 บันทึกกุญแจรหัสส่วนตัวลงในอุปกรณ์ที่สามารถพกพาได้ เช่นบันทึกลงในสมาร์ทการ์ดโดยอาจผนวกเทคโนโลยีของ Biometric เข้ามาใช้ด้วย	ผู้บริหาร
	4.2.8 ผู้บริหารต้อง รักษากุญแจรหัสส่วนตัวที่ใช้งานในลักษณะเดียวกับบัตรเครดิตหรือบัตร เอ.ที.เอ็ม ถ้าพบว่าสูญหายหรือชำรุดต้องรีบทำการแจ้งทางเจ้าหน้าที่ที่เกี่ยวข้องทันที	ผู้บริหาร

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
	5.0 การตรวจสอบและประเมินความเสี่ยงด้านการใช้งาน	
	จุดประสงค์ : เพื่อตรวจสอบระบบหรือลดความเสี่ยงภัยจากจุดอ่อนที่อาจเกิดขึ้นและป้องกันการหยุดชะงักในการดำเนินงานที่เป็นผลมาจากความล้มเหลวของการให้บริการด้านต่างๆของระบบ	
5.1	ควรมีการบันทึกเหตุการณ์เพื่อใช้ตรวจสอบระบบดังนี้	
	5.1.1 การเข้าใช้งานเครื่องให้บริการต่างๆ	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	5.1.2 การเข้าใช้งานเครื่องปฏิบัติการ	เจ้าหน้าที่ปฏิบัติงาน
	5.1.3 การจัดการข้อมูลที่เกี่ยวกับเจ้าหน้าที่รับลงทะเบียนและผู้ขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	5.1.4 การจัดการกุญแจและใบรับรอง	เจ้าหน้าที่ปฏิบัติงาน
	5.1.5 การเพิกถอนใบรับรองและการออกรายการเพิกถอนใบรับรอง	เจ้าหน้าที่ปฏิบัติงาน
	5.1.6 การเปิด-ปิด เครื่องและโปรแกรมที่ทำหน้าที่ในการลงลายมือชื่ออิเล็กทรอนิกส์ ในใบรับรองให้กับผู้ขอใช้บริการ	เจ้าหน้าที่ปฏิบัติงาน
	5.1.7 การจัดการฐานข้อมูล	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	5.1.8 การปรับปรุงเปลี่ยนแปลงค่าของระบบ บันทึกเก็บค่าเก่าไว้ด้วย	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	5.1.9 การปรับปรุงด้านฮาร์ดแวร์และซอฟต์แวร์	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
	5.1.10 การบำรุงรักษาระบบคอมพิวเตอร์และสถานที่ติดตั้งระบบ	เจ้าหน้าที่ปฏิบัติงาน
	5.1.11 การให้บริการผ่านอินเตอร์เน็ต	เจ้าหน้าที่ปฏิบัติงาน
	5.1.12 การเข้าขอใช้บริการไดเร็กทอรี่	เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนปฏิบัติงาน	ผู้ปฏิบัติ หรือ ผู้รับผิดชอบ
5.2	มีระบบป้องกันการอ่านการบันทึกและมีขั้นตอนกฎเกณฑ์การบันทึก	เจ้าหน้าที่ปฏิบัติงาน
5.3	มีการเปิดเผยมาตรการป้องกันการเข้าถึง	หัวหน้างานระบบสารสนเทศ / ผู้ดูแลระบบ
5.4	ตรวจสอบการดักจักข้อมูลทางคอมพิวเตอร์เช่น Key Stroke	เจ้าหน้าที่ปฏิบัติงาน
5.5	เกิดการปลอมแปลงทางคอมพิวเตอร์และมีเนื้อหาที่ไม่เหมาะสม เช่น	
	5.5.1 ข้อมูลคอมพิวเตอร์เพื่อให้ผู้อื่นเชื่อว่าข้อมูลนั้นเป็นของบุคคลที่สามหรือมาจากหรือจัดทำโดยบุคคลที่สาม	เจ้าหน้าที่ปฏิบัติงาน
	5.5.2 ข้อมูลคอมพิวเตอร์ที่เป็นเท็จ	เจ้าหน้าที่ปฏิบัติงาน
	5.5.3 ข้อมูลที่ไม่เหมาะสม เช่น ข้อมูลก่อให้เกิดความไม่สงบ มีลักษณะลามกอนาจาร	เจ้าหน้าที่ปฏิบัติงาน
5.6	ตรวจสอบการป้องกันการบุกรุกด้วยวิธีต่างๆที่ใช้ในปัจจุบันซึ่งมีการโจมตีดังตัวอย่างรูปที่ 3.1	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน

ตารางที่ 3.2 ขั้นตอนการได้มา การใช้งานและการดูแลรักษากุญแจรหัสส่วนตัว

ในขั้นตอนการปฏิบัติงานเพื่อความปลอดภัยนั้นขึ้นอยู่กับระดับความสำคัญของการใช้งานถ้าระบบที่ต้องการความปลอดภัยในระดับที่สูงสุดขั้นตอนการปฏิบัติก็จะมีขั้นตอนที่ต้องปฏิบัติมากขึ้นด้วยแต่ถ้าในหน่วยงานหรือองค์ที่ไม่ได้มีข้อมูลที่สำคัญก็เลือกขั้นตอนบางข้อในการปฏิบัติได้ซึ่งขั้นตอนการปฏิบัติที่ควรมีในองค์กรหรือหน่วยงานที่เป็นพื้นฐานที่สำคัญเพื่อความปลอดภัยได้แสดงไว้ในตารางที่ 3.2 มาตรฐานที่จำเป็นพื้นฐาน

มาตรฐานที่จำเป็นพื้นฐาน		
ลำดับที่	**ขั้นตอนการปฏิบัติงาน**	**ผู้รับผิดชอบ**
1.0	ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษรและนโยบายนี้ต้องได้รับการอนุมัติจากผู้บริหารขององค์กรในการนำไปใช้	ผู้บริหาร
2.0	ต้องทำการติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร	ผู้บริหาร / หัวหน้างานสารสนเทศ
3.0	ต้องกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศในคุณสมบัติของบุคลากรที่ต้องการสรรหา	หัวหน้างานสารสนเทศ
4.0	ต้องตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรองประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ หรือการผ่านการอบรม เป็นต้น	หัวหน้างานสารสนเทศ
5.0	ต้องทำรายงานเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยซึ่งเกิดขึ้นให้แก่ผู้ที่รับผิดชอบทราบโดยเร่งด่วน	เจ้าหน้าที่ปฏิบัติงาน
6.0	ต้องรายงานจุดอ่อน ช่องโหว่ หรือภัยที่พบในระบบสารสนเทศที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน	เจ้าหน้าที่ปฏิบัติงาน
7.0	ต้องรายงานการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟแวร์ที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน	เจ้าหน้าที่ปฏิบัติงาน
8.0	ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยหรือระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัยขององค์กร	ผู้บริหาร
9.0	ต้องมีการจัดสรรพื้นที่ หรือ จัดทำกำแพง หรือ ผนังที่มีความแข็งแรงเพื่อล้อมรอบบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย	หัวหน้างานสารสนเทศ

ลำดับที่	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ
10	ต้องมีการควบคุมการเข้าออกในบริเวณพื้นที่ควบคุมโดยให้ผ่านเข้า-ออกได้เฉพาะผู้ที่มีสิทธิเท่านั้น	หัวหน้างานสารสนเทศ
11	ต้องมีมาตรการควบคุมบริเวณที่จัดไว้ให้เป็นที่สำหรับการส่งมอบโดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดไว้ ทั้งนี้เพื่อป้องกันการเข้าถึงระบบจากผู้ที่ไม่ได้รับอนุญาต	หัวหน้างานสารสนเทศ
12	ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ เช่น คอมพิวเตอร์หรือระบบที่มีความสำคัญต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานหรือห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตูหน้าต่างของสำนักงานต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่ และต้องตั้งเครื่องโทรสารหรือถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น	หัวหน้างานสารสนเทศ
13	ต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัย รวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์นั้น	เจ้าหน้าที่ปฏิบัติงาน
14	ต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรองไว้ด้วย เช่นการเดินสายไฟสำรองใช้ Uninterruptible Power Supply ใช้เครื่องปั่นไฟสำรองเป็นต้น	หัวหน้างานสารสนเทศ
15	ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้า หรือ สายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดิน ผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย เป็นต้น	หัวหน้างานสารสนเทศ
16	ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ	หัวหน้างานสารสนเทศ

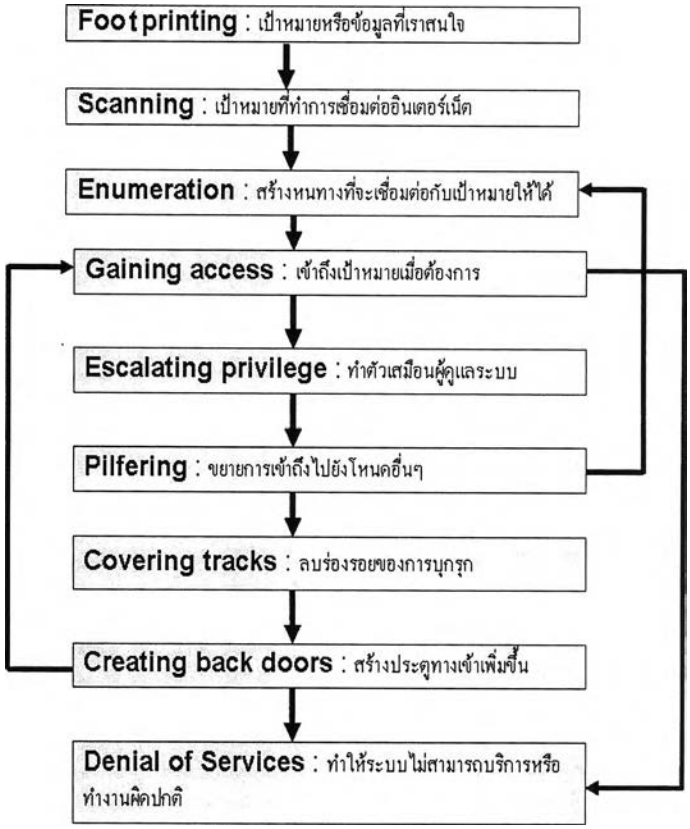
ลำดับที่	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ
17	ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญๆ ไว้ในที่ที่สามารถพบเห็นได้ง่ายโดยจัดเก็บไว้ในที่ที่ปลอดภัย ต้องทำการลงบันทึกออกจากเครื่องคอมพิวเตอร์ (Log off) เมื่อจำเป็นต้องหยุดการใช้งานคอมพิวเตอร์ไปเป็นระยะเวลาหนึ่ง นอกจากนี้ ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย	เจ้าหน้าที่ปฏิบัติงาน
18	ต้องกำหนดให้มีการควบคุมการนำ อุปกรณ์เอกสาร ซอฟแวร์ หรือทรัพย์สินอื่นๆขององค์กรออกนอกสำนักงานอย่างมั่นคงปลอดภัย	เจ้าหน้าที่ปฏิบัติงาน
19	ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือละเมิดความมั่นคงปลอดภัย ได้แก่ ระบบไม่สามารถให้บริการได้ ความผิดพลาดอาจเกิดจากข้อมูลที่คีย์เข้าระบบไม่ถูกต้อง การเปิดเผยข้อมูลความลับขององค์กรหรือระบบขัดข้อง เป็นต้น	หัวหน้างานสารสนเทศ
20	ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่ายเพื่อให้เกิดความชัดเจนในการปฏิบัติหน้าที่และลดการทุจริตในการปฏิบัติหน้าที่	หัวหน้างานสารสนเทศ
21	ต้องมีการติดตั้งและใช้งานซอฟแวร์ป้องกันไวรัส หนอน และ ม้าโทรจัน เพื่อป้องกันความเสียหายของข้อมูล รวมทั้งมีกลไกเพื่อสร้างความตระหนักให้แก่ผู้ใช้ภายในองค์กร และดูแลมาตรการป้องกันให้ทันสมัยอยู่เสมอ	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
22	ต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสม เช่น สำรองข้อมูลอย่างน้อย 1 ครั้งในรอบ 6 เดือน และในการจัดเก็บข้อมูลสำรองควรจัดให้สถานที่จัดเก็บที่เตรียมไว้เท่านั้น	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
23	ต้องมีการบริหารและจัดการด้านความมั่นคงปลอดภัยบนเครือข่าย ดังต่อไปนี้	ผู้ดูแลระบบ

ลำดับที่	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ
	23.1 การกำหนดหน้าที่ความรับผิดชอบในการดูแลอย่างชัดเจน 23.2 มีวิธีการในการป้องกันข้อมูลที่ต้องส่งผ่านออกไปยังอินเตอร์เน็ตโดยเฉพาะป้องกันความลับและความสมบรูณ์ของข้อมูล 23.3 มีกลไกโครงสร้างที่สนับสนุนสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่อง	
24	ต้องจัดทำระเบียบปฏิบัติในการใช้งานไปรษณีย์อิเล็กทรอนิกส์ ทางด้าน 24.1 การป้องกันไวรัสคอมพิวเตอร์ หนอนอินเตอร์เน็ต และม้าโทรจัน 24.2 การป้องกันข้อความและไฟล์แนบที่มีความสำคัญด้วยการเข้ารหัส 24.3 การไม่ใช้ไปรษณีย์อิเล็กทรอนิกส์ในการส่งเอกสารสำคัญเพื่อป้องกันปัญหาการลักลอบการขโมยหรืออ่านข้อมูล 24.4 การไม่ส่งไปรษณีย์อิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดสิทธิส่วนบุคคล หรือใช้ในทางไม่เหมาะสม เป็นต้น	หัวหน้างานสารสนเทศ
25	ต้องกำหนดวิธีการปฏิบัติที่ดีในการเลือกใช้งานรหัสผ่าน การยกเลิก และการเปลี่ยนแปลงรหัสผ่าน	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
26	ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล	เจ้าหน้าที่ปฏิบัติงาน
27	ต้องกำหนด ให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาติให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสานสนเทศขององค์กรได้	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
28	ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้พนักงานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน

ลำดับที่	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ
29	ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับพนักงานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้ระบบงาน	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
30	ต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการบางอย่างเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะทำการปฏิเสธการเข้าใช้งานเมื่อผู้ใช้บริการป้อนรหัสผ่านผิดเกิน 3 ครั้งเป็นต้น	ผู้ดูแลระบบ
31	ต้องกำหนดให้ระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้พนักงานเปลี่ยนรหัสตามระยะเวลาที่กำหนด	ผู้ดูแลระบบ
32	ต้องจัดให้มีการควบคุมการกำหนดสิทธิในการใช้งานระบบสารสนเทศ เช่น ความสามารถในการเข้าถึงข้อมูล การเปลี่ยนแปลงแก้ไขข้อมูล การกำหนดสิทธิของกลุ่มผู้ใช้งานได้และตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน	ผู้ดูแลระบบ
33	ต้องกำหนดให้มีการบันทึกการเข้าใช้งานระบบสารสนเทศซึ่งข้อมูลที่เก็บ ได้แก่ ผู้ใช้งาน เวลาที่เข้าและออกจากระบบ ต้นทางมาจากแอดเดรสใดบนเครือข่าย รวมทั้งการเก็บนี้ต้องเก็บไว้เป็นช่วงระยะเวลาหนึ่งที่เหมาะสม	ผู้ดูแลระบบ
34	ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอิงเวลาจากมาตรฐานโลก เพื่อช่วยให้การตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก	ผู้ดูแลระบบ
35	ต้องกำหนดระยะเวลาที่เหมาะสมเพื่อตรวจสอบข้อมูลกิจกรรมการเข้าใช้งานที่ได้บันทึกเก็บไว้ เช่น กำหนดระยะเวลา 3 หรือ 6 เดือน ตามความถี่ที่เหมาะสม เป็นต้น	หัวหน้างานสารสนเทศ
36	ต้องกำหนดความต้องการด้านความปลอดภัยให้ชัดเจนในระบบที่จะพัฒนาขึ้นมาหรือซื้อมาใช้งาน	หัวหน้างานสารสนเทศ

ลำดับที่	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ
37	ต้องตรวจสอบข้อมูลนำเข้าระบบสารสนเทศ ได้แต่ ตรวจสอบช่วงของค่าตัวเลขที่ใส่เข้ามาตรวจสอบแต่ละตัวอักษรที่ใส่เข้ามา ตรวจว่าข้อมูลที่ใส่เข้ามาครบทุกฟิลด์ เป็นต้น	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
38	ต้องมีการควบคุมการติดตั้งซอฟแวร์ใหม่ ซอฟแวร์ไลบรารี่ ซอฟแวร์อุดช่องโหว่ลงไปยังเครื่องที่ใช้งานหรือเครื่องที่ให้บริการ ทั้งนี้ก่อนการติดตั้งต้องผ่านการทดสอบมาเป็นอย่างดีว่าจะไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่นั้น	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
39	39 ต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟแวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือให้บริการอยู่แล้วซึ่งได้แก่ 3.6.39.1 คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ 3.6.39.2 ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ 3.6.39.3 ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากการแก้ไข 3.6.39.4 เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ 3.6.39.5 ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน
40	ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟแวร์อย่างเคร่งครัดและมีการควบคุมการใช้งานซอฟแวร์ตามลิขสิทธ์ที่ได้รับด้วย ได้แก่การจดทะเบียนเพื่อใช้งานซอฟแวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ตรวจสอบอย่างสม่ำเสมอว่าซอฟแวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่	ผู้ดูแลระบบ / เจ้าหน้าที่ปฏิบัติงาน

ตารางที่ 3.3 **มาตรการที่จำเป็นพื้นฐาน** [21]



รูปที่ 3.1 **โครงสร้างของการบุกรุก** (Anatomy of Hack) [20]

ขั้นตอนการปฏิบัติต่างๆที่ได้นำเสนอนั้นเป็นเครื่องมือในการใช้งานแต่ในการที่จะให้ผู้บริหารได้รับรู้ข้อมูลข่าวสารนั้นวิธีหรือขั้นตอนในการนำเสนอเป็นสิ่งที่สำคัญการให้ข้อมูลข่าวสารเป็นสิ่งแรกที่ให้ผู้บริหารได้รับรู้หรือนำไปพิจารณาในประโยชน์เพื่อเป็นขั้นตอนของการนำไปสู่การยอมรับและนำขั้นตอนปฏิบัติงานนี้ไปทดลองใช้งาน

แนวทางในการเสนอเพื่อให้ผู้บริหารยอมรับเพื่อการนำไปใช้งาน

จากทฤษฎีและการนำเสนอแนวความคิดต่างๆ ในเรื่องของกระบวนการยอมรับและกระบวนการตัดสินใจ พอจะสรุปเป็นแนวทางในการนำเสนอให้ผู้บริหาร ได้ดังนี้

3.7.1 ต้องมีการนำเสนอผู้บริหารในแง่ของการเปรียบเทียบให้เห็นว่ามีองค์กรหรือหน่วยงานที่มีความสำคัญในระดับเดียวกันหรือสูงกว่า ได้ดำเนินงานหรือปฏิบัติงานด้านความปลอดภัยด้วยวิธีการลักษณะเดียวกัน และผู้บริหารในระดับสูงขององค์กรนั้นได้ให้การยอมรับและนำไปใช้งานจริงทำให้ผู้บริหารได้เกิดความยอมรับที่จะเรียนรู้หรือทดลองการใช้งาน

3.1.2 การนำเสนอให้ทำความรู้จัก วิธีการและหลักการ ตลอดจน ข้อมูลข่าวสารทางด้านการใช้งานและเหตุผลของความจำเป็นที่ต้องมีขั้นตอนในการปฏิบัติในการใช้งานกุญแจรหัสส่วนตัว

3.1.3 การจูงใจ ต้องสร้างแรงจูงใจในการใช้งานแม้ว่า การสร้างทัศนคติที่ชอบหรือไม่ชอบของผู้บริหารนั้นจะเป็นขั้นความรู้เป็นเรื่องของความคิดหรือการรู้ ส่วนการจูงใจเป็นเรื่องของอารมณ์หรือความรู้สึก ซึ่งจะทำให้ผู้บริหารแสวงหาแหล่งข่าวสารข้อมูล แสวงหาสาระข่าวข้อมูลที่รับมาเกี่ยวกับนวัตกรรมนับว่าเหมาะสมกับตัวเขาทั้งในสภาพปัจจุบันและในอนาคตหรือไม่อย่างไร การจูงใจเป็นขั้นตอนของกระบวนการตัดสินใจ ในการยอมรับในการนำเสนอเพื่อการใช้งานที่จะเกิดขึ้นและเมื่อผู้บริหารต้องการเปลี่ยนแปลงสภาพเดิมที่มีอยู่แต่ยังมีความไม่แน่ใจในสิ่งที่นำเสนอและอาจมีความรู้สึกเกี่ยวกับสิ่งที่นำเสนอนั้นเป็นผลมาจากการรับรู้คุณค่าของสิ่งนั้นดังนั้นขั้นจูงใจจึงสอดคล้องกับขั้นการประเมินหรือพิจารณาทางเลือกในขั้นตอนกระบวนการตัดสินใจทั่วไป

3.1.4 การนำนวัตกรรมไปใช้งานนั้น กระบวนการตัดสินใจยอมรับนวัตกรรมในขั้นตอนต้นๆเป็นเรื่องของความรู้ ความคิดแต่การนำไปใช้เป็นเรื่องของการปฏิบัติ เมื่อบุคคลตัดสินใจที่จะยอมรับนวัตกรรมนั้นไปใช้ เขาต้องรู้ว่าเขาสามารถได้นวัตกรรมนั้นมาจากไหน นวัตกรรมนั้นใช้อย่างไร เมื่อนำไปใช้จะประสบปัญหาอย่างไรและสามารถแก้ปัญหานั้นได้อย่างไร จึงต้องให้ผู้บริหารทราบว่า ขั้นตอนการปฏิบัติงานที่ได้นำเสนอนั้นมีพื้นฐานความเป็นมาอย่างไรและมาจากมาตรฐานที่เป็นที่ยอมรับกันทั่วโลกในการนำไปใช้งาน

3.1.5 ต้องลดความสลับซับซ้อนของขั้นตอนการปฏิบัติลงในการใช้งานของผู้บริหารและต้องความสามารถที่จะทดลองได้ สามารถแยกส่วนไปทดลองใช้ได้ ซึ่งจะช่วยให้ผู้บริหารมีความรู้สึกเสี่ยงน้อยลง การยอมรับจะมากกว่าที่ไม่อาจทดลองได้ในขอบเขตจำกัดนอกจากนั้นควรจัดบุคลากรอาวุโสของฝ่ายสารสนเทศให้รับผิดชอบในการฝึกอบรมแบบถ่ายทอดทักษะเป็นการส่วนตัวหรือเป็นกลุ่มเล็กๆให้แก่ผู้บริหาร ทั้งนี้ด้วยเหตุผลที่จะช่วยโน้มน้าวผู้บริหาร และลดทอนความรู้ด้านเทคนิคที่ไม่จำเป็น

3.1.6 ต้องทำให้ผู้บริหารเห็นได้ว่าการนำไปใช้นั้นเห็นผลได้ง่ายและผลนั้นแสดงออกชัดเจน เข้าใจง่าย ซึ่งจะทำให้ผู้บริหารจะยอมรับได้ง่ายและรวดเร็วกว่า เช่นทดลองในการส่งอิเล็กทรอนิกส์เมล์แล้วการเข้าด้วยรหัสกุญแจส่วนตัวเพื่อยืนยันผู้ส่ง และการปลอมถอดรหัสนั้นจำเป็นต้องใช้เวลาและอุปกรณ์คอมพิวเตอร์ที่มีประสิทธิภาพสูง เพื่อให้ผู้บริหารเชื่อถือ เป็นต้น

ขั้นตอนการปฏิบัติงานต่างๆเป็นขั้นตอนในการสร้างความปลอดภัยทั้งด้านการสร้างกุญแจรหัส การเตรียมการ เป็นเพียงแนวทางที่ควรปฏิบัติหรือ Best practice เท่านั้นในการ

ปฏิบัติงานจริงอาจต้องมีการปรับเปลี่ยนเพื่อความเหมาะสมอีกทั้งยังมีปัจจัยด้านบุคลากรที่มีความชำนาญตลอดจนเทคโนโลยีด้านความปลอดภัยที่พัฒนาเปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้นในบทต่อไปจะเป็นการนำขั้นตอนที่ได้มาแยกประเภทของการนำไปใช้ซึ่งสามารถแยกได้เป็น 2 ประเภทคือขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ทั่วไป กับ ขั้นตอนการปฏิบัติของผู้บริหารตลอดจนแสดงปัจจัยและข้อควรปฏิบัติในการนำเสนอวิธีการปฏิบัติดังกล่าวต่อผู้บริหารเพื่อการยอมรับนำไปใช้งานในหน่วยงานหรือองค์กรของตน