บทที่ 4

ผลการวิจัย

จากการวิจัยโดยนำมาตรฐาน ISO/IEC17799, CobiT, ITIL และ HIPPAA มาใช้โดยอาศัยสภาพแวดล้อมของจุฬาลงกรณ์มหาวิทยาลัยเพื่อรองรับการใช้งานกุญแจรหัสส่วนตัวนั้น พบว่า การได้มาและการใช้งานกุญแจรหัสส่วนตัวเป็นเพียงขั้นตอนหนึ่งของขั้นตอนทั้งหมด การได้มาเพื่อนำไปใช้งานกุญแจรหัสส่วนตัวนั้น ต้องมีขั้นตอนหรือกระบวนการต่างๆที่ครอบคลุมเช่น นโยบายด้านความปลอดภัยของการนำเทคโนโลยีกุญแจคู่สาธารณะมาใช้ การเตรียมการพื้นฐานต่างๆเพื่อสร้างความปลอดภัยในการรองรับการสร้างกุญแจรหัสส่วนตัว

ขั้นตอนหรือกระบวนการต่างๆที่ได้จากการใช้วิธีการศึกษาและอ้างอิงโดยเปรียบเทียบจากมาตรฐานด้านความปลอดภัยที่ยอมรับในระดับสากลซึ่งมีการนำไปใช้งานอย่างแพร่หลายเช่น ISO, COBIT, ITIL และ HIPPAA ที่ได้ในบทที่ 3 นั้น ผู้ทำวิจัยเห็นว่าในการนำใช้งานจริงนั้นไม่สามารถใช้งานได้อย่างเหมาะสมกับผู้ใช้งานในทุกระดับได้โดยเฉพาะผู้บริหาร เช่น ผู้บริหารระดับตั้งแต่รองอธิการบดีขึ้นไปอาจมีความไม่สะดวกในการปฏิบัติตามขั้นตอนบางขั้นตอนหรือระเบียบทุกอย่างได้ ดังนั้นจึงจัดรูปแบบของขั้นตอนในการปฏิบัติในการ สร้าง การใช้งาน และการดูแลรักษา โดยได้กำหนดแนวทางในการปฏิบัติได้เป็น 2 รูปแบบคือ

1. ขั้นตอนปฏิบัติงานสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป
2. ขั้นตอนปฏิบัติงานสำหรับผู้บริหาร

โดยมีการนำเสนอขั้นตอนการปฏิบัติงานในรูปแบบของตารางดังต่อไปนี้

ขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานทั่วไป	
ลำดับที่	**ขั้นตอนปฏิบัติงาน**
	1.0 นโยบายด้านความปลอดภัย (Security Policy)
1.1	จัดทำ เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร
1.2	ต้องมีการจัดทำบัญชีทรัพย์สินที่มีทั้งหมดในองค์กร
1.3	สามารถทำการตรวจสอบติดตามทรัพย์สินต่างๆที่มีในองค์ได้ ว่าอยู่ที่ใดสถานะเป็นอย่างไร และมีข้อมูลรายละเอียดต่างๆของทรัพย์สินนั้น
1.4	ต้องจัดให้มีมาตรการรักษาความปลอดภัยให้กับห้องทำงานตลอดจนเครื่องมืออุปกรณ์ต่างๆ
1.5	ป้องกันพื้นที่ ให้มีความปลอดภัย ต้องมีการจัดสรรพื้นที่ให้สามารถดูแลด้านความปลอดภัยได้อย่างทั่วถึง
1.6	การสร้างสิ่งขวางกั้นเพื่อกำหนดบริเวณความปลอดภัย
1.7	เตรียมพื้นที่ในการส่งมอบวัสดุหรือผลิตภัณฑ์ต่างๆ โดยจัดแยกเป็นพื้นที่ในการส่งมอบแยกออกจากพื้นที่ควบคุมสำคัญ
1.8	การควบคุมการเข้า-ออก บริเวณองค์กร
1.9	การสร้างห้องสำหรับสร้างกุญแจรหัสลับ
1.10	เตรียมการสำรองการใช้ไฟฟ้า
1.11	ทำการคงอุณหภูมิให้มีความเหมาะสมต่อการปฏิบัติงาน
1.12	มีการวางแผนการปรับปรุงอุปกรณ์ต่างๆเพื่อให้ทันสมัยและมีประสิทธิภาพ
1.13	ต้องทำรายงานเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยซึ่งเกิดขึ้นให้แก่ผู้ที่รับผิดชอบทราบโดยเร่งด่วน

ลำดับที่	ขั้นตอนปฏิบัติงาน
1.14	ต้องรายงานจุดอ่อน ช่องโหว่ หรือภัยที่พบในระบบสารสนเทศที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน
1.15	ต้องรายงานการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟแวร์ที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน
1.16	จัดให้มีสายล่อฟ้าป้องกันกรณีฟ้าผ่าและมีการเดินสายดิน
1.17	การป้องกันภัยจากน้ำ
	2.0 สถานใช้สร้างกุญแจรหัสส่วนตัว
2.1	การติดตั้งโทรทัศน์วงจรปิด เพื่อบันทึกเหตุการณ์
2.2	ติดตั้งระบบการป้องกันผู้บุกรุกโดยไม่ได้รับอนุญาต
2.3	ติดตั้งเครื่องดักจับความสั่นสะเทือนหรือการถูกโจรกรรม
2.4	การตรวจสอบการเปิด ปิดของประตูมีสัญญาณเตือนภัยส่งเสียงเมื่อประตูของห้องที่สำคัญๆไม่ถูกปิด
2.5	การตรวจสอบควันที่อาจเกิดจาก อัคคีภัย หรือ สารระเหย ไวไฟ
2.6	การป้องกันการบุกรุกจากภายใต้ห้องปฏิบัติการหรือใต้ดิน
2.7	ติดตั้งสารดับเพลิงที่ไม่ทำลายอุปกรณ์สำคัญๆ
2.8	การเตรียมการป้องกันอุปกรณ์สำคัญต่างๆนั้นไว้กรณีเกิดไฟไหม้
	3.0 การควบคุมการเข้าถึง และ ใช้งานอุปกรณ์ต่างๆทางกายภาพ
3.1	การเข้าหรือ ออก พื้นที่ควบคุมให้เฉพาะผู้มีสิทธิเท่านั้น
3.2	บันทึกภาพด้านหน้าตรงของบุคคลที่เข้าออก
3.3	มีการควบคุมบุคคลที่เข้าออกด้วยการทดสอบตั้งแต่สองชนิดขึ้นไป

ลำดับที่	ขั้นตอนปฏิบัติงาน
3.4	ไม่ติดตั้งเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อทางเครือข่าย
3.5	ต้องล็อคหรือใส่กุญแจทุกห้องที่ไม่มีผู้ปฏิบัติงานอยู่
3.6	ไม่มีการอนุญาตให้มีการบันทึกต่างๆ เช่น วีดีโอ กล่องถ่ายรูป
3.7	อุปกรณ์การทำสำเนาทุกชนิด ต้องใช้เจ้าหน้าที่เป็นผู้ดำเนินการ
3.8	ไม่มีการขนย้ายใดๆจากในองค์กรออกสู่ภายนอกโดยไม่ได้รับอนุญาต ต้องมีเอกสารรับรองการขนย้ายหรือนำสิ่งของ
3.9	ต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง
3.10	กำหนดให้มีการพิสูจน์ตัวตนสำหรับพนักงานในการเข้าปฏิบัติงาน
3.11	ตั้งเวลาในเครื่องคอมพิวเตอร์ให้ตรงกันและเทียบกับเวลามาตรฐานกลางของโลก
3.12	ควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
3.13	ทำการบันทึกรายละเอียดการเข้าใช้งานโปรแกรมและยูทิลิตี้
3.14	เตรียมการจัดเก็บสื่อบันทึกต่างๆในสถานที่ปลอดภัย
3.15	มีการจัดเก็บบันทึกการเข้าใช้งานระบบ
3.16	สื่อบันทึกข้อมูลในรูปแบบต่างๆต้องถูกทำลายจนแน่ว่าไม่สามารถจะกู้คืนมาได้
	4.0 ทรัพยากรบุคคล
4.1	บุคลากรทุกคนต้องปฏิบัติตามงานภายใต้ข้อกำหนดระเบียบวิธีปฏิบัติ
4.2	กำหนดให้มีกฎระเบียบการลงโทษต่อการฝ่าฝืน หรือละเมิดนโยบาย
4.3	ต้องรายงานให้ผู้ที่รับผิดชอบทราบทันทีที่พบสิ่งผิดปกติ

ลำดับที่	ขั้นตอนปฏิบัติงาน
4.4	ห้ามนำอุปกรณ์ไปใช้ผิดประเภท
4.5	บันทึกการทำงานและประวัติการทำงาน การซ่อมบำรุง ของอุปกรณ์
4.6	เครื่องมือหรืออุปกรณ์ต่างๆ เจ้าหน้าที่ไม่สามารถนำเข้ามาปฏิบัติได้
4.7	ทำสัญญาลงนามในการรักษาความลับที่สำคัญ และการเปิดเผยข้อมูล
4.8	วัดความรู้ความสามารถในส่วนที่ต้องรับผิดชอบของงาน
4.9	ทดสอบทัศนคติ อารมณ์ การแก้ปัญหา การทดสอบทางจิตวิทยา
4.10	ตรวจสอบประวัติของบุคลากร ประวัติอาชญากรรม ประวัติการทำงาน
4.11	ตรวจสอบสุขภาพ เช่น โรคติดต่อที่ร้ายแรง
4.12	กำหนดหน้าที่ความรับผิดชอบของงานให้กับผู้ที่จะรับผิดชอบทราบ
4.13	ต้องไม่มีการรับผิดชอบในตำแหน่งที่สำคัญด้วยบุคลากรเพียงคนเดียว
4.14	ในการปฏิบัติงานต้องมีการจัดทำบัญชีตารางในการทำงาน
4.15	เจ้าที่ปฏิบัติงานทุกคน ต้องผ่านกระบวนการตรวจสอบตัวตนของเจ้าหน้าที่นั้น และมีการบันทึกรายละเอียดการเข้าทำงานอย่างชัดเจน
4.16	จัดให้มีการฝึกอบรมเทคโนโลยี หรือความรู้ใหม่ๆด้านความมั่นคง
4.17	จัดประชุมทบทวนนโยบายความปลอดภัย กฎระเบียบ
4.18	ดูงาน ฝึกอบรมการรับมือต่อเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคง
4.19	การทำรายงาน การแจ้งเหตุ ตลอดจนวิธีการสังเกตสิ่งผิดปกติ
4.20	ทดสอบความสามารถในการปฏิบัติงานของเจ้าหน้าที่เป็นประจำ

ลำดับที่	ขั้นตอนปฏิบัติงาน
4.21	การจัดทำคู่มือหรือเอกสารการใช้งานและดูแลรักษาอุปกรณ์ต่างๆ
	5.0 ใบรับรองอิเล็กทรอนิกส์และกุญแจรหัสส่วนตัว
5.1	ให้บริการและจัดการด้านเครื่องคอมพิวเตอร์สำหรับ ระบบให้บริการใบรับรองในด้านต่างๆ
5.2	บริหารจัดการระบบจัดเก็บข้อมูลของระบบให้บริการใบรับรอง
5.3	รับคำขอใช้บริการ
5.4	ออกใบรับรองให้กับผู้ขอใช้บริการ
5.5	รับคำขอเพิกถอนใบรับรอง
5.6	เพิกถอนใบรับรองตามคำร้องขอของผู้ใช้บริการ
5.7	พิสูจน์ความถูกต้องและตัวตนของผู้ขอใช้บริการ
5.8	การเผยแพร่ใบรับรองอิเล็กทรอนิกส์
5.9	การเรียกคืนใบรับรองอิเล็กทรอนิกส์
5.10	แจ้งข้อมูลข่าวสาร ความเคลื่อนไหว การเปลี่ยนแปลง ให้กับที่ผู้มีส่วนเกี่ยวข้องในข้อมูลที่กระทบต่อสิทธิ หน้าที่
5.11	อำนวยความสะดวกให้แต่ผู้ขอใช้บริการ
5.12	มีวิธีการเก็บข้อมูลเอกสารหลักฐานในสถานที่ที่ปลอดภัย
5.13	มีการประกาศถ้อยแถลงในแนวทางขั้นตอนการออกใบรับรอง
5.14	การควบคุมดูแล บริหารจัดการงานที่สำคัญต้องมีผู้รับผิดชอบในตำแหน่งดังกล่าวอย่างน้อย 2 คน ที่รับรู้
5.15	การเปลี่ยนแปลงแก้ไขกุญแจของระบบต้องกำหนดให้มีผู้รับผิดชอบอย่างน้อย 3 ร่วมกันรับผิดชอบ

ลำดับที่	ขั้นตอนปฏิบัติงาน
5.16	การทำงานต่างๆต้องมีหลักฐานที่สามารถสืบย้อนได้
5.17	แสดงหลักฐานและเอกสารคำร้องขอสร้างกุญแจรหัสส่วนตัวในกรณีต้องการสร้างกุญแจรหัสส่วนตัว
5.18	เมื่อผ่านการตรวจสอบเอกสารเจ้าหน้าที่จะทำการนัดเพื่อสร้างกุญแจรหัสส่วนตัว
5.19	ในการเข้าไปห้องปฏิบัติการจะมีระเบียบและข้อบังคับต่างๆให้ปฏิบัติ
5.20	ผู้สร้างรหัสต้องเป็นผู้ดำเนินการตั้งแต่ต้นจนจบ
5.21	ในกระบวนการสร้างกุญแจคู่สาธารณะนั้น กุญแจรหัสส่วนตัวที่สัมพันธ์กับกุญแจสาธารณะ นั้นจะต้องมอบให้ผู้สร้างทันทีหลังจากเสร็จกระบวนการ
5.22	ส่งกุญแจสาธารณะ ชื่อที่แตกต่าง (Distinguished name) และชื่อทั่วไป (Common name) ให้แก่องค์กรที่จะใช้บริการ
5.24	กรอกแบบฟอร์มข้อมูลและ เอกสารต่างๆที่ผู้ให้บริการร้องขอ
5.25	การส่งต้องแน่ใจว่ามีความปลอดภัย โดยอาจเข้ารหัสด้วยกุญแจสาธารณะขององค์กรที่ต้องการขอใบรับรอง เป็นต้น
5.26	เมื่อเอกสารต่างๆผ่านการพิจารณาแล้ว องค์กรที่รับรองออกใบรับรองให้ จะประกอบด้วยกุญแจสาธารณะของผู้ขอและข้อมูลอื่นๆที่เกี่ยวข้อง โดยองค์กรนั้นจะรับรองโดยการลงลายมือชื่ออิเล็กทรอนิกส์ กับความถูกต้องส่งมาด้วย
5.27	ใบรับรองบุคคลหรือเครื่องลูกข่าย 1 กรอกแบบฟอร์มข้อมูลที่องค์กรต้องการพร้อมทั้งจัดส่งข้อมูลที่ร้องขอเช่น บัตรประจำตัวประชาชน จัดส่งด้วยช่องทางที่ปลอดภัย 2 รอการตรวจสอบเอกสารและการยืนยัน 3 ทำสัญญากับองค์กรรับรอง 4 นำไปใช้งานตามเงื่อนไขที่ทางองค์กรรับรองแจ้งให้ทราบ

ลำดับที่	ขั้นตอนปฏิบัติงาน
	6.0 แนวทางการป้องกันกุญแจรหัสส่วนตัว
6.1	การกำหนดมาตรฐานขั้นต่ำ โดยเปรียบเทียบกับมาตรฐานการรักษาความปลอดภัย
6.2	ทำการตรวจสอบระบบ เพื่อประทำการประเมินความเสี่ยงของช่องโหว่ต่างๆของระบบ (Vulnerability Assessment)
6.3	ตรวจสอบระบบ (Audit) ตลอดจนอุปกรณ์เครือข่ายและอุปกรณ์
6.4	เก็บข้อมูลที่ได้จากการตรวจสอบ (Inventory) ให้เป็นระบบ
6.5	ทำการประเมินความเสี่ยงจากข้อมูลที่ได้จากการทดสอบ
6.6	ทำการปิดความเสี่ยงภัยที่ประเมินได้ เช่นการปรับเปลี่ยนรหัส
6.7	นำระบบหรือเทคโนโลยีด้านความปลอดภัยมาเสริมสนับสนุนตรวนสอบ
6.8	ปรับปรุง Patch หรือนำระบบ Patch Management System มาใช้งาน
6.9	ทำการตรวจสอบติดตามด้านความปลอดภัยอยู่เสมอ
6.10	ล็อคเครื่องคอมพิวเตอร์ (Computer Lock)
6.11	ติดตั้งรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนตัว
6.12	ล็อคหน้าจอคอมพิวเตอร์ (Screen Lock)
6.13	ล็อคไฟล์ต่างๆที่มีลักษณะดังนี้คือ 6.13.1 ล็อคไฟล์ที่ไม่สมบรูณ์หรือขาดหายไป 6.13.2 ล็อคไฟล์ที่มี Timestamp ผิดปกติ 6.13.3 ล็อคไฟล์ที่มี Permission เช่นการล็อคไฟล์ระบบที่เจ้าของ เป็น user

ลำดับที่	ขั้นตอนปฏิบัติงาน
	6.13.4 ข้อมูลของการรีบูตเครื่องหรือการทำการรีสตาร์ท Service 6.13.5 การใช้คำสั่ง su หรือการ login เข้ามาจากต้นทางที่ผิด 6.13.6 ไม่มอบหมายให้ผู้อื่นผู้ใดกระทำธุรกรรมอิเล็กทรอนิกส์โดยใช้กุญแจรหัสของตน 6.13.7 ไม่นำกุญแจรหัสไปใช้งานในสภาพแวดล้อมที่ขาดความน่าเชื่อถือ 6.13.8 ตรวจสอบการดูการเปลี่ยนแปลงของความปลอดภัยทาง กายภาพที่เกิดขึ้น (Detecting Physical Security Compromises) 6.13.9 ไม่เปิดการใช้งานบริการต่างๆที่ไม่สำคัญเช่น ftp, telnet, finger 6.13.10 ต้องมีความระมัดระวังกุญแจรหัสของตนเสมือนของที่มีค่าสำคัญ 6.13.11 เมื่อมีข้อสงสัยหรือพิรุธที่สังเกตเห็น ต้องทำการแจ้งให้กับ ผู้มีส่วนเกี่ยวข้องรับผิดชอบทันที 6.13.12 ไม่เปิดเผยข้อมูลใดๆของตนให้กับเว็บไซต์หรือบุคคลอื่นใดที่ไม่มีความน่าเชื่อถือ
6.14	ตั้งรหัสผ่านในการเข้าสู่ระบบให้ยากต่อการคาดเดา
6.15	ทำการเปลี่ยนกุญแจรหัสใหม่ทันที่เมื่อเกิดเหตุการณ์ดังนี้ 6.15.1 มีการขโมยรหัสหรือทำซ้ำ 6.15.2 สูญหายหรือใช้การไม่ได้ 6.15.3 มีผู้อื่นล่วงรู้กุญแจส่วนตัว 6.15.4 มีการเปลี่ยนแปลงข้อมูลในใบรับรอง 6.15.5 มีการยกเลิกการใช้งาน 6.15.6 ต้องการเปลี่ยนรหัสใหม่

ลำดับที่	ขั้นตอนปฏิบัติงาน
	6.15.7 มีปัญหาการถูกโจมตีหรือเจาะระบบของผู้ให้บริการออก
6.16	ตรวจสอบประเมินความเสี่ยงด้านการใช้งาน 6.16.1 การเข้าใช้งานเครื่องให้บริการต่างๆ 6.16.2 การเข้าใช้งานเครื่องปฏิบัติการ 6.16.3 การจัดการข้อมูลที่เกี่ยวกับเจ้าหน้าที่รับลงทะเบียนและผู้ขอใช้บริการ 6.16.4 การจัดการกุญแจและใบรับรอง 6.16.5 การเพิกถอนใบรับรองและการออกรายการเพิกถอนใบรับรอง 6.16.6 การเปิด-ปิด เครื่องและโปรแกรมที่ทำหน้าที่ในการลงลายมือชื่อ 6.16.7 การจัดการฐานข้อมูล 6.16.8 การปรับปรุงเปลี่ยนแปลงค่าของระบบ บันทึกเก็บค่าเก่าไว้ด้วย 6.16.9 การปรับปรุงด้านฮาร์ดแวร์และซอฟต์แวร์ 6.16.10 การบำรุงรักษาระบบคอมพิวเตอร์และสถานที่ติดตั้งระบบ 6.16.11 การให้บริการผ่านอินเตอร์เน็ต 6.16.12 การเข้าขอใช้บริการไดเร็กทอรี่ 6.16.13 มีระบบป้องกันการอ่านการบันทึกและมีขั้นตอนกฎเกณฑ์การบันทึก 6.16.14 มีการเปิดเผยมาตรการป้องกันการเข้าถึง 6.16.15 มีการดักจักข้อมูลทางคอมพิวเตอร์เช่น Key Stroke

ลำดับที่	ขั้นตอนปฏิบัติงาน
	6.16.16 เกิดการปลอมแปลงทางคอมพิวเตอร์และมีเนื้อหาที่ไม่เหมาะสม เช่น 6.16.17 ข้อมูลคอมพิวเตอร์ที่เป็นเท็จ 6.16.18 ข้อมูลที่ไม่เหมาะสม เช่น ข้อมูลก่อให้เกิดความไม่สงบ

ขั้นตอนการปฏิบัติงานสำหรับผู้บริหาร

ลำดับที่	ขั้นตอนปฏิบัติงาน
	1.0 นโยบายด้านความปลอดภัย (Security Policy)
1.1	จัดทำ เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร
1.2	สนับสนุน และส่งเสริมเพื่อให้ระบบสามารถดำเนินการ โดยอยู่ภายใต้แผนงานที่ได้กำหนด
1.3	ผู้บริหารองค์กร ต้องกำหนดบทบาทหน้าที่ความรับผิดชอบ
1.4	ต้องจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยให้พนักงานทุกระดับในองค์ที่ต้องมีส่วนเกี่ยวข้องทราบ
1.5	ต้องเลือกหน่วยงานที่ออกใบรับรองอิเล็กทรอนิกส์ที่ใช้กันทั่วโลกที่สามารถใช้ในการทำธุรกรรมด้านการเงินอิเล็กทรอนิกส์ที่มีมูลค่ามหาศาลได้
1.6	ต้องมีการให้สรุปสาระสำคัญของความรู้ข่าวสารความเคลื่อนไหวให้รับทราบอยู่เสมอ

ลำดับที่	ขั้นตอนปฏิบัติงาน
	2.0 การสร้างรหัสกุญแจส่วนตัว
2.1	ใช้อุปกรณ์ที่มีการเตรียมไว้สร้างกุญแจรหัส เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆที่ใช้ในการสร้างรหัสกุญแจส่วนตัว
2.2	ต้องมีความระมัดระวังในการควบคุมการเข้าออกในบริเวณที่จัดไว้ให้ เช่นไม่เปิดประตูทิ้งไว้ ไม่นำบุคคลอื่นเข้าไปด้วย
2.3	เป็นผู้ดำเนินการในการสร้างกุญแจรหัสในเครื่องคอมพิวเตอร์และอุปกรณ์ที่เตรียมไว้ตั้งแต่ต้นจนจบ กรณีที่มีข้อสงสัยในการปฏิบัติจะมี วีดีโอ ที่เจ้าหน้าที่ได้เตรียมไว้แล้วคอยแนะนำให้ผู้บริหารสามารถปฏิบัติตามขั้นตอนไปพร้อมๆกันได้
2.4	กุญแจรหัสส่วนตัวที่สัมพันธ์กับกุญแจสาธารณะ นั้นจะต้องรับมอบทันทีหลังจากเสร็จกระบวนการโดยอาจอยู่ในรูปของ Smart Card ซึ่งอาจมีการตั้งรหัสผ่านในการที่จะ Active โดยอาจมีการใช้เทคนิคของ Token keys of key มาเสริม
2.5	กุญแจสาธารณะของผู้บริหารจะนำไปขอใบรับรองอิเล็กทรอนิกส์โดยอยู่ภายใต้การรับรู้และความเข้าใจของผู้บริหาร
	3.0 การดูแลรักษากุญแจรหัสของผู้บริหาร
3.1	มีเจ้าหน้าที่รับผิดชอบดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์ที่ใช้งานของผู้บริหาร ต้องจัดให้มีมาตรการรักษาความปลอดภัยให้กับห้องทำงานตลอดจนเครื่องมืออุปกรณ์ต่างๆของผู้บริหาร
3.2	การใช้งานเครื่องคอมพิวเตอร์ส่วนตัวของผู้บริหารจะทำการกรอง MAC Address ที่กำหนดค่าที่ระบุให้ใช้โดยการกำหนดตารางที่อนุญาตและไม่อนุญาต ตลอดจนติดตั้งระบบความปลอดภัยในเครื่องผู้บริหารด้วย
3.3	ผู้บริหารต้องไม่นำกุญแจรหัสส่วนตัวไปใช้งานในสถานที่ที่ไม่แน่ใจถึงความปลอดภัยเช่น เว็บไซต์ทั่วไป
3.4	บันทึกกุญแจรหัสส่วนตัวลงในอุปกรณ์ที่สามารถพกพาได้ เช่นบันทึกลงในสมาร์ทการ์ดโดยอาจผนวกเทคโนโลยีของ Biometric เข้ามาใช้ด้วย
3.5	ผู้บริหารต้อง รักษากุญแจรหัสส่วนตัวที่ใช้งานในลักษณะเดียวกับบัตรเครดิตหรือบัตร เอ.ที.เอ็ม ถ้าพบว่าสูญหายหรือชำรุดต้องรีบทำการแจ้งทางเจ้าหน้าที่ที่เกี่ยวข้องทันที

ลำดับที่	ขั้นตอนปฏิบัติงาน
3.6	ต้องล็อคหรือใส่กุญแจทุกห้องที่ไม่มีผู้ปฏิบัติงานอยู่
3.7	การใช้งานทุกครั้งต้องระมัดระวังตามสมควรแก่สถานการณ์
3.8	ติดตั้งระบบการป้องกันผู้บุกรุกโดยไม่ได้รับอนุญาต เช่นสัญญาณเตือนภัยในห้องทำงาน
3.9	มีการมีการควบคุมการเข้าออกห้องผู้บริหาร การทดสอบตั้งแต่สองชนิดขึ้นไปเช่น Biometric + Smart Cart หรือ รหัสผ่านประตู + บัตรประจำตัว + กุญแจประตู
3.10	ต้องทำการแจ้งแก่เจ้าหน้าที่ที่เกี่ยวข้องทันทีเมื่อ 3.10.1 รู้สึกมีความไม่ถูกต้องเกี่ยวกับกุญแจรหัสส่วนตัวหรือไม่มีความมั่นใจในกุญแจรหัสส่วนตัว 3.10.2 มีผู้อื่นล่วงรู้กุญแจส่วนตัว 3.10.3 มีการเปลี่ยนแปลงข้อมูลในใบรับรอง 3.10.4 ต้องการยกเลิกการใช้งาน 3.10.5 ต้องการเปลี่ยนรหัสใหม่ 3.10.6 ชำรุดหรือเกิดความเสียหายหรือใช้งานไม่ได้
3.11	ไม่มอบหมายให้ผู้หนึ่งผู้ใดกระทำธุรกรรมแทนตนโดยมอบรหัสกุญแจส่วนตัวของผู้บริหารนั้นๆให้กระทำการแทน
3.12	ต้องเข้าใจถึงวิธีการใช้งานที่ถูกต้องและปลอดภัยจากข้อมูลข่าวสารที่นำเสนอจากหน่วยงานที่เกี่ยวข้องอย่างเคร่งครัด
3.13	ไม่บอกถึงวิธีการในการใช้งาน รูปแบบของกุญแจรหัส ให้แก่ผู้หนึ่งผู้ใดทั้งสิ้น
3.14	ในกรณีที่ใช้ในรูปบัตรพกพา ไม่พกพาแบบเปิดเผย หรือไม่ระมัดระวังในการพกพา และ ปฏิบัติตามวิธีการใช้งานอย่างเคร่งครัด