

6.5 แนวทางการจัดทำขั้นตอนการปฏิบัติงาน (IT Procedure) [7]

การจัดทำขั้นตอนการปฏิบัติงานเทคโนโลยีสารสนเทศในระดับต่างๆ บุคลากรในกรมฯ และศูนย์เทคโนโลยีสารสนเทศ ควรจะร่วมมือกันประเมินผลกระทบด้านต่างๆ โดยเฉพาะด้านประสิทธิผลของงาน ด้านประสิทธิภาพของระบบ และด้านความมั่นคงปลอดภัยของข้อมูล ทั้งในด้านบวกและลบ การเพิ่ม/ลดความซับซ้อน การเพิ่ม/ลดความปลอดภัย จำเป็น/ไม่จำเป็น เร่งด่วน/ไม่เร่งด่วน เป็นต้น ดังตัวอย่างในตารางที่ 6.5.1 ซึ่งขั้นตอนการปฏิบัติงานการรักษาความมั่นคงปลอดภัยของข้อมูลโดยละเอียดจะกล่าวในหัวข้อที่ 6.6 ต่อไป

ตารางที่ 6.5.1 การประเมินผลกระทบด้านประสิทธิผล ด้านประสิทธิภาพและด้านความมั่นคงปลอดภัยของข้อมูลต่อขั้นตอนการปฏิบัติงานต่างๆ ของระบบสารสนเทศ

หมายเหตุ “-” หมายถึง มีผลกระทบน้อยมาก

ขั้นตอนการปฏิบัติงาน/ ผลกระทบ	ด้านประสิทธิผล ของงาน	ด้านประสิทธิภาพ ของระบบ	ด้านความมั่นคง ปลอดภัยของข้อมูล
ด้านข้อมูล (Data)			
มาตรฐานพิกัดตำแหน่ง	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
มาตรฐานชนิดข้อมูลต่างๆ	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การสำรองข้อมูลส่วนกลาง	บวก	เพิ่มความซับซ้อน	จำเป็น/เร่งด่วน
การสำรองข้อมูลส่วนตัว	-	-	จำเป็น/ไม่เร่งด่วน
การแชร์ข้อมูล	บวก	-	จำเป็น/ไม่เร่งด่วน
ด้านบุคลากร (Personnel)			
การบริหารจัดการผู้ใช้	-	เพิ่มความซับซ้อน	จำเป็น/เร่งด่วน
การฝึกอบรมและการทดสอบ	บวก	บวก	จำเป็น/เร่งด่วน
การล็อกอินก่อนเข้าใช้งาน	-	เพิ่มความซับซ้อน	จำเป็น/เร่งด่วน
การเปลี่ยนรหัสผ่าน (Password) บ่อยๆ	-	เพิ่มความซับซ้อน	จำเป็น/เร่งด่วน
ด้านอุปกรณ์ (Hardware)			
มีความปลอดภัยตาม พระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การทดแทนอุปกรณ์ที่อายุมาก	จำเป็น/เร่งด่วน	บวก	จำเป็น/ไม่เร่งด่วน
การซ่อมบำรุงอุปกรณ์	เร่งด่วน	-	-

ขั้นตอนการปฏิบัติงาน/ ผลกระทบ	ด้านประสิทธิผล ของงาน	ด้านประสิทธิ ภาพของระบบ	ด้านความมั่นคง ปลอดภัยของข้อมูล
การนำอุปกรณ์ส่วนตัวมาใช้งาน ในองค์กร	เร่งด่วน	-	จำเป็น/เร่งด่วน
การนำอุปกรณ์จากหน่วยงาน อื่นๆ มาใช้งานในองค์กร	-	-	จำเป็น/เร่งด่วน
การติดตามและควบคุมการใช้	ไม่เร่งด่วน	-	จำเป็น/ไม่เร่งด่วน
การควบคุมปริมาณอุปกรณ์	ไม่เร่งด่วน	-	จำเป็น/ไม่เร่งด่วน
ด้านซอฟต์แวร์ (Software)			
มีความปลอดภัยตาม พระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การจัดหาระบบสารสนเทศใหม่	จำเป็น	บวก	จำเป็น/เร่งด่วน
การบำรุงรักษาระบบ สารสนเทศ	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การติดตั้งซอฟต์แวร์ลิขสิทธิ์	จำเป็น/ไม่เร่งด่วน	บวก	จำเป็น/เร่งด่วน
การต่ออายุซอฟต์แวร์ลิขสิทธิ์ บางประเภท	จำเป็น/เร่งด่วน	บวก	จำเป็น/เร่งด่วน
การติดตั้งซอฟต์แวร์ละเมิด ลิขสิทธิ์เพื่อปฏิบัติงาน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การใช้ซอฟต์แวร์นอกเหนือจาก งานที่ได้รับมอบหมาย	ลบ	ลบ	จำเป็น/เร่งด่วน
การใช้ข้อมูล/เว็บไซต์เพื่อความ บันเทิง	ลบ	ลบ	จำเป็น/เร่งด่วน
ด้านเครือข่าย (Network)			
ปฏิบัติตามพระราชบัญญัติว่า ด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
มีความปลอดภัยตาม พระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน

ขั้นตอนการปฏิบัติงาน/ ผลกระทบ	ด้านประสิทธิผล ของงาน	ด้านประสิทธิ ภาพของระบบ	ด้านความมั่นคง ปลอดภัยของข้อมูล
การเข้าถึงทางเครือข่ายจาก ภายนอกสู่ภายใน	จำเป็น/ไม่เร่งด่วน	-	จำเป็น/เร่งด่วน
การเข้าถึงทางเครือข่ายจาก ภายในสู่ภายนอก	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การเปิด/ปิดการใช้เครือข่ายใน บางช่วงเวลา	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การเปิด/ปิดการใช้เครือข่ายใน บางเว็บไซต์ในบางช่วงเวลา	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การเปิด/ปิดการใช้เครือข่ายใน บางพอร์ท (Port) ในบาง ช่วงเวลา	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การแชร์ไฟล์ผ่านระบบ P2P	จำเป็น/เร่งด่วน	ลบ	จำเป็น/เร่งด่วน
การควบคุมการใช้งานเครือข่าย อินเทอร์เน็ตบนอุปกรณ์บางตัว	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
ด้านขั้นตอนการทำงาน (Procedure)			
มีความปลอดภัยตาม พระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน	จำเป็น/เร่งด่วน
การวางแผนเมื่อเกิดภัยพิบัติ	จำเป็น/ไม่เร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน
การร่วมกันร่างขั้นตอนการ ปฏิบัติงานด้วยกันภายในกรมฯ	จำเป็นเร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน
ขั้นตอนการจัดหาอุปกรณ์ เพิ่มเติม	จำเป็น/เร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน
ลำดับขั้นตอนการตัดสินใจใน สถานการณ์ปกติและฉุกเฉิน	จำเป็น/ไม่เร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน
การตอบสนองต่อสถานการณ์ ฉุกเฉิน	จำเป็น/ไม่เร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน
การกู้คืนระบบ	จำเป็น/ไม่เร่งด่วน	จำเป็น/ไม่เร่งด่วน	จำเป็น/เร่งด่วน

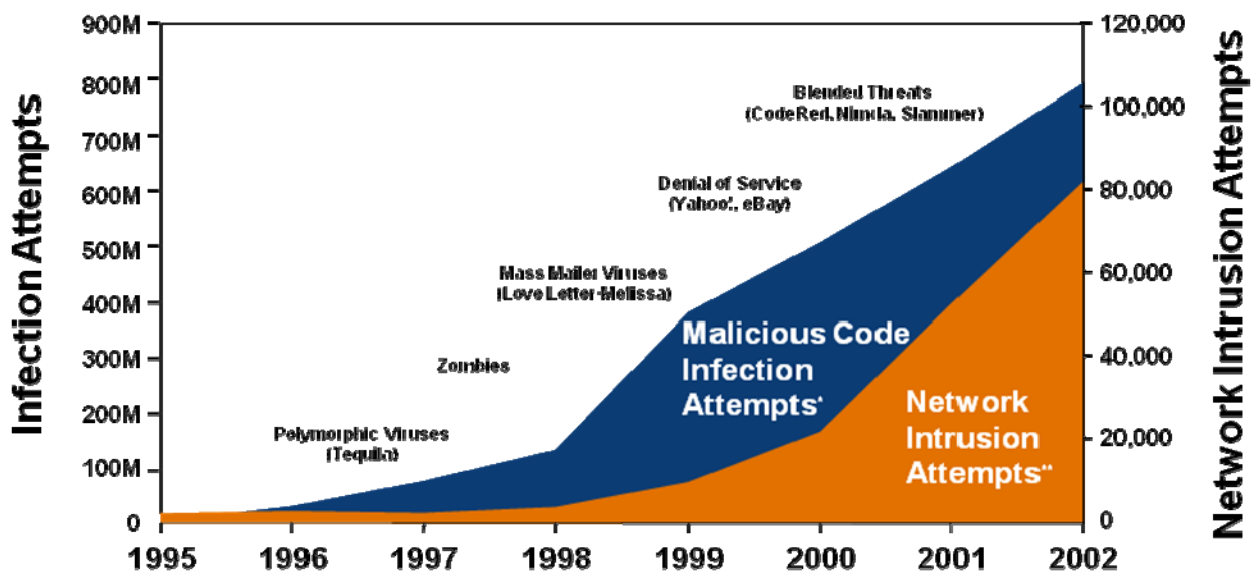
การจัดทำขั้นตอนการปฏิบัติงานการใช้เทคโนโลยีสารสนเทศดังตัวอย่างข้างต้น มีประเด็นที่สามารถเพิ่มเติมได้เพื่อให้ครอบคลุมระดับกรมฯ ระดับสำนัก ระดับส่วน และระดับบุคคล ซึ่งจำเป็นต้องมีเจ้าหน้าที่ซึ่งเป็นตัวแทนของศูนย์เทคโนโลยีสารสนเทศ มีส่วนร่วมในการกำหนดขั้นตอนการปฏิบัติงานทุกระดับ เพื่อให้เป็นไปในทิศทางเดียวกันและเป็นต้นแบบให้ศูนย์เทคโนโลยีสารสนเทศ และบุคลากรของกรมฯ ช่วยกันปรับปรุงต่อไป โดยจะต้องเริ่มต้นจัดทำขั้นตอนการปฏิบัติงานที่มีความจำเป็น/เร่งด่วน จากตารางที่ 6.5.1 ส่วนขั้นตอนการปฏิบัติงานด้านอื่นๆ สามารถทยอยจัดทำและปรับปรุงทุกๆ 6 เดือน ส่วนขั้นตอนการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูลจะกล่าวต่อไป

6.6 แนวทางการจัดทำขั้นตอนการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูล (IT Security Procedure) [3]

หัวข้อนี้จะกล่าวถึงปัญหาและที่มาของขั้นตอนการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศทั้งหมดของกรมฯ โดยจะเน้นหัวข้อที่มีความสำคัญและจำเป็น/เร่งด่วน เพื่อให้สามารถป้องกันและบรรเทาผลกระทบจากการโจมตี/การบุกรุกที่รุนแรงและซับซ้อนได้ ดังนั้น การกำหนดขั้นตอนการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูล จะต้องมีความคิดในเชิงรุกเพื่อป้องกันการเกิดของปัญหาและสอดคล้องกับภาพรวมและการทำงานของบุคลากรภายในกรมฯ อย่างมีประสิทธิภาพ

6.6.1 ปัญหาและที่มา

การโจมตีในอดีต ปัจจุบัน และอนาคตมีความซับซ้อนเพิ่มมากขึ้น จากรูปที่ 6.6.1 และ 6.6.2 การโจมตีทางบุคคลหรือผู้ใช้เป็นส่วนที่เพิ่มขึ้น ผ่านทาง Social Network เช่น Facebook.com เป็นต้น จะเห็นได้ว่าแนวโน้มของการโจมตี (บุกรุก) จากเครือข่ายอินเทอร์เน็ตมีสัดส่วนมากกว่าการติดไวรัส และมีแนวโน้มเพิ่มมากขึ้นเรื่อยๆ

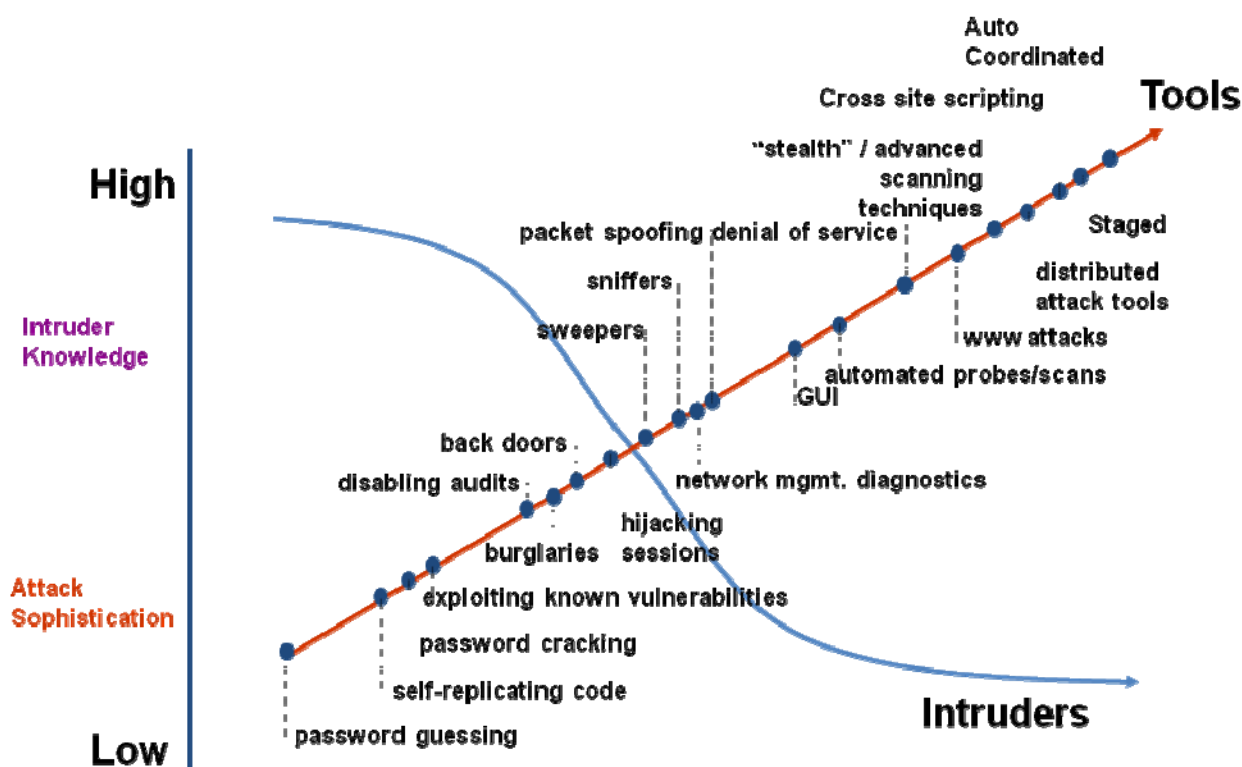


*Analysis by Symantec Security Response using data from Symantec, IDC & ICSA, 2002 estimated

**Source: CERT

รูปที่ 6.6.1 จำนวนการกระจายตัว (Infection Attempts) ไวรัสคอมพิวเตอร์และ
จำนวนการบุกรุก (Intrusion Attempts) ระหว่างปี ค.ศ. 1995-2002

การบุกรุกทางเครือข่ายจากภายนอกกรมฯผ่านทางเครือข่ายอินเทอร์เน็ตจะต้องอาศัยความรู้ และความสามารถของผู้บุกรุกรวมถึงการใช้เครื่องมือที่ซับซ้อน (Sophistication) มากขึ้น ดังนั้น ขั้นตอนการปฏิบัติงาน แผน และเครื่องมือรักษาความมั่นคงปลอดภัยของข้อมูล จึงเป็นหัวใจสำคัญของระบบสารสนเทศชนิด Web Application ในปัจจุบัน



รูปที่ 6.6.2 ความรู้ของผู้บุกรุก (Intruder Knowledge) และความซับซ้อนของการโจมตี (Attack Sophistication) มีแนวโน้มเพิ่มขึ้น โดยอาศัยจำนวนผู้บุกรุก (Intruders) น้อยลง

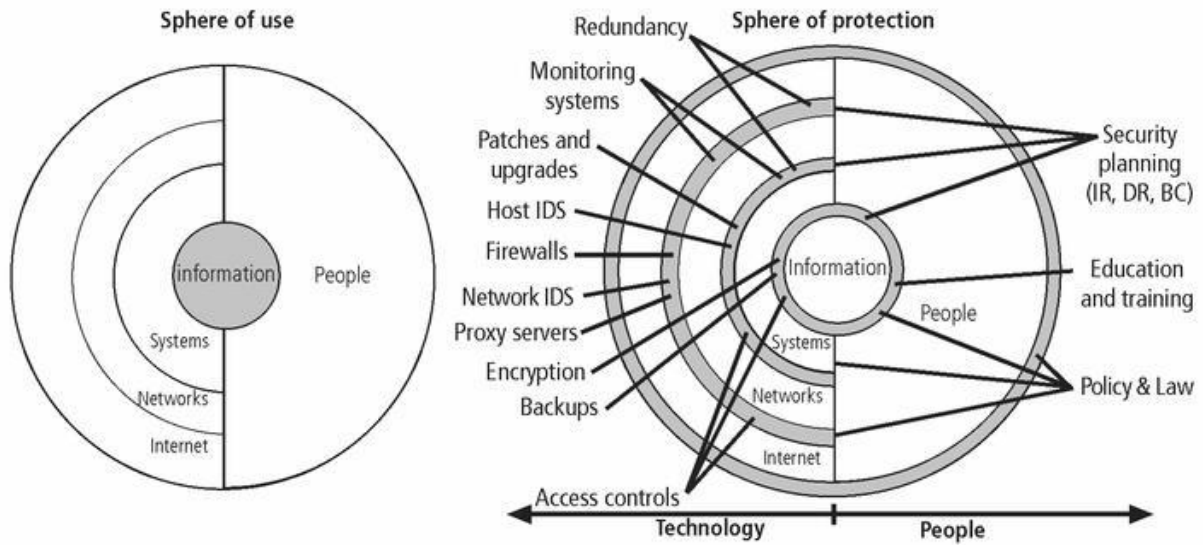
จากผลการวิเคราะห์ในบทที่ 4 พบว่า “มากกว่า 50% ของเครื่องคอมพิวเตอร์ทั้งในส่วนกลางและส่วนภูมิภาค ไม่มีการอัปเดตระบบป้องกันและตรวจจับไวรัส” ปัญหานี้เป็นการสะสมที่เกิดจากหลายสาเหตุ ยกตัวอย่างเช่น จำนวน License ของระบบป้องกันไวรัสไม่เพียงพอ การติดตั้งระบบซอฟต์แวร์ในเครื่องลูกข่ายไม่เป็นเอกภาพ เป็นต้น

การป้องกันและแก้ปัญหาควรมีขั้นตอนการปฏิบัติงานที่ครบถ้วน เพื่อให้ผู้ปฏิบัติงานมองปัญหาได้รอบด้านและเป็นระบบ ยกตัวอย่างเช่น

- การนำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ด้าน ICT มาติดตั้งใช้ในเครือข่าย ไม่มีขั้นตอนการปฏิบัติงาน กฎและข้อปฏิบัติที่ชัดเจน ทำให้เปิดช่องโหว่ของการโจมตีได้โดยไม่ตั้งใจ
- อุปกรณ์ที่เก่า การอัปเดตระบบปฏิบัติการและซอฟต์แวร์อื่น หรือการต่ออายุสิทธิ์การใช้งาน (License) จำเป็นต้องตั้งงบประมาณรองรับ เพื่อจัดหาอุปกรณ์มาทดแทน อัปเดต และต่ออายุสิทธิ์การใช้งาน
- อื่นๆ

จึงเป็นที่มาของขั้นตอนการปฏิบัติงานเพื่อความมั่นคงปลอดภัยของข้อมูลในหัวข้อนี้ ซึ่งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ ควรจะต้องกำหนดหรือจัดทำร่วมกันกับตัวแทนของสำนัก/หน่วยงานต่างๆ ภายในกรมฯ โดยหัวข้อนี้จะกล่าวถึง ทฤษฎีเบื้องต้นในการจัดทำเพื่อเป็นแนวทางในการจัดทำขั้นตอนการปฏิบัติงาน

และแผนในระดับกรมฯ ภายใต้หลักการที่เรียกว่า **ทรงกลมของการใช้งาน** (Sphere of Use) และ**ทรงกลมของการป้องกัน** (Sphere of Protection) ซึ่งมีความสอดคล้องกันดังรูปที่ 6.6.3



รูปที่ 6.6.3 ทรงกลมของการใช้งาน (Sphere of Use) และ ทรงกลมของการป้องกัน (Sphere of Protection) แหล่งที่มา: [3]

ทรงกลมของการใช้งาน จะห่อหุ้มข้อมูล/สารสนเทศสารสนเทศอยู่ด้านใน โดยมีชั้นต่างๆ ดังนี้

- ชั้นการเข้าถึงระบบ (Systems) ซึ่งมีบุคลากร (People) ที่เข้าถึงระบบได้น้อย
- ชั้นการเข้าถึงเครือข่าย (Networks) ซึ่งหมายถึง เครือข่ายอินเทอร์เน็ตภายในองค์กร และ
- ชั้นนอกสุด คือ เครือข่ายอินเทอร์เน็ต ซึ่งมีขอบเขตหรือพื้นที่ผิวกว้างขวาง ซึ่งครอบคลุมผู้คนจำนวนมากที่ประสงค์ดีและไม่ประสงค์ดีปะปนกันไป

ทรงกลมของการป้องกัน จะห่อหุ้มข้อมูล/สารสนเทศอยู่ด้านในสุด โดยมีอุปกรณ์หรือกลไกในชั้นต่างๆ ป้องกันไว้ ดังนี้

- ชั้นการเข้าถึงสารสนเทศ (Information)
 - ด้านเทคโนโลยีสามารถป้องกันได้โดยการเข้ารหัส (Encryption) การสำรอง (Backup) การทำซ้ำ (Redundancy) การควบคุมการเข้าถึง (Access Control)
 - ด้านบุคลากร (People) ซึ่งเข้าถึงระบบได้เพิ่มขึ้น จะต้องใช้กลไกของการร่างขั้นตอนการปฏิบัติงานและกฎหมาย (Policy & Law) และการวางแผนรับมือกับสถานการณ์ต่างๆ เช่น การกู้คืนเมื่อเกิดเหตุการณ์ (IR: Incident Recovery) การกู้คืนเมื่อเกิดภัยพิบัติ (DR: Disaster Recovery) และการดำเนินธุรกิจอย่างต่อเนื่อง (BC: Business Continuity) เมื่อกู้คืนระบบได้แล้ว
- ชั้นการเข้าถึงระบบ (Systems)

- ด้านเทคโนโลยีสามารถป้องกันได้โดย การทำซ้ำ (Redundancy) ระบบเฝ้าระวัง (Monitoring systems) การควบคุมการเข้าถึง (Access Control) ระบบตรวจจับการโจมตีของเครื่องแม่ข่าย (Host IDS) การแพตช์และอัปเดต (Patches and upgrades)
- ด้านบุคลากร (People) ซึ่งมีจำนวนน้อยที่เข้าถึงระบบได้ จะต้องใช้กลไกของการศึกษาและการฝึกอบรม (Education and Training) การร่างขั้นตอนการปฏิบัติงานและกฎหมาย (Policy & Law) และการวางแผนรับมือกับสถานการณ์ต่างๆ เช่น การกู้คืนเมื่อเกิดเหตุการณ์ (IR: Incident Recovery) การกู้คืนเมื่อเกิดภัยพิบัติ (DR: Disaster Recovery) และการดำเนินธุรกิจอย่างต่อเนื่อง (BC: Business Continuity) เมื่อกู้คืนระบบได้แล้ว
- ขั้นการเข้าถึงเครือข่ายภายใน (Networks)
 - ด้านเทคโนโลยีสามารถป้องกันได้โดย ระบบเฝ้าระวัง (Monitoring systems) ไฟร์วอลล์ (Firewall) ระบบตรวจจับการโจมตีผ่านเครือข่าย (Network IDS) การใช้พร็อกซีเซิร์ฟเวอร์ (Proxy Server) การควบคุมการเข้าถึง (Access Control)
 - ด้านบุคลากร (People) ซึ่งมีจำนวนน้อยที่เข้าถึงระบบได้ จะต้องใช้กลไกการร่างขั้นตอนการปฏิบัติงานและกฎหมาย (Policy & Law) และการวางแผนรับมือกับสถานการณ์ต่างๆ เช่น การกู้คืนเมื่อเกิดเหตุการณ์ (IR: Incident Recovery) การกู้คืนเมื่อเกิดภัยพิบัติ (DR: Disaster Recovery) และการดำเนินธุรกิจอย่างต่อเนื่อง (BC: Business Continuity) เมื่อกู้คืนระบบได้แล้ว
- ขั้นการเข้าถึงเครือข่ายภายนอกทางเครือข่ายอินเทอร์เน็ต (Internet)
 - ด้านเทคโนโลยีเองสามารถป้องกันได้บ้าง เช่น การยืนยันตัวตน (Authentication) การล็อกอิน (Log In) การตอบคำถามที่เคยป้อนคำตอบไว้แล้ว (Challenge/Response) การกรอกตัวอักษรที่อ่านยากขึ้น (Captcha) การป้องกันการโจมตีด้วยชุดคำสั่งหรือสคริปต์ (Script) การใช้ใบประกาศดิจิทัล (Digital Certificate) เป็นต้น
 - ด้านบุคลากร (People) ซึ่งมีจำนวนน้อยที่เข้าถึงระบบได้ จะต้องใช้กลไกการร่างขั้นตอนการปฏิบัติงานและกฎหมาย (Policy & Law) เป็นหลักซึ่งในประเทศไทย คือ พ.ร.บ. การใช้คอมพิวเตอร์ปี พ.ศ. 2550

6.6.2 ขั้นตอนการปฏิบัติงานและแผนความมั่นคงปลอดภัยของข้อมูล

เพื่อให้สอดคล้องกับขั้นตอนการปฏิบัติงานเทคโนโลยีสารสนเทศ การจัดทำขั้นตอนการปฏิบัติงานและแผนความมั่นคงปลอดภัยของข้อมูล จึงแบ่งเป็นด้านข้อมูล ด้านบุคลากร ด้านอุปกรณ์ ด้านซอฟต์แวร์ ด้านเครือข่ายและด้านขั้นตอนการทำงาน ดังตารางที่ 6.6.1

ตารางที่ 6.6.1 ขั้นตอนการปฏิบัติงานและแผนความมั่นคงปลอดภัยของข้อมูล

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
ด้านข้อมูล (Data)		
มาตรฐานพิกัดตำแหน่งในกรมฯ	กรมฯ ควรจะมีมาตรฐานของพิกัดตำแหน่งและข้อมูลเดียว เพื่อให้สอดคล้องกับแผนแม่บท GIS แห่งชาติ	ศทส นักธรณี และนักภูมิสารสนเทศ ควรช่วยกันกำหนดมาตรฐานของพิกัดตำแหน่งและข้อมูลที่สอดคล้องกับแผนแม่บท GIS แห่งชาติ
มาตรฐานชนิดข้อมูลต่างๆ	-----”-----	-----”-----
การสำรองข้อมูลส่วนกลาง	จะต้องมีการสำรองข้อมูลของกรมฯ เป็นระยะๆ	จัดเตรียมพื้นที่หน่วยความจำภายนอกให้เพียงพอ และมีการเข้ารหัส หรือทำ Message Digest เพื่อป้องกันการแก้ไข
การสำรองข้อมูลส่วนตัว	ผู้ใช้แต่ละคนควรจะต้องจัดหาพื้นที่ในการสำรองข้อมูลเอง	ใช้ระบบ Rollback เพื่อไม่ให้เครื่องเก็บข้อมูลอื่นของผู้ใช้ได้เลย
การแชร์ข้อมูล	ผู้ใช้แต่ละคนควรจะต้องแชร์ข้อมูลเท่าที่จำเป็น	จัดหาพื้นที่ส่วนกลางให้กับผู้ใช้แต่ละคนในการแชร์ข้อมูลโดยจำกัดพื้นที่ไม่เกินคนละ 200 เมกะไบต์
ด้านบุคลากร (Personnel)		
การบริหารจัดการผู้ใช้	เจ้าหน้าที่ของกรมฯ จะต้องมีการแสดงตัวตน เพื่อเข้าถึงสถานที่ปฏิบัติงาน เป็นต้น ผู้ใช้ทุกคนจะต้องล็อกอินเพื่อยืนยันตัวตนทุกคน	ระบบฐานข้อมูลผู้ใช้งานจะต้องระบุหมายเลขบัตร การเข้าถึงห้องหรือสถานที่สำคัญจะต้องใช้บัตรแสดงตัวตน และมีการลงบันทึกเก็บประวัติ
การฝึกอบรมและการทดสอบ	ผู้ใช้ทุกคนจะต้องผ่านการฝึกอบรมด้านความปลอดภัยในหลักสูตร บ.5 ในบทที่ 13	เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้จัดการฝึกอบรมและประเมินผู้เข้ารับ
การล็อกอินก่อนเข้าใช้งาน	ระบบจะต้องเข้มแข็งและผู้ใช้ต้องไม่ล็อกอินแทนกัน	มีการเปลี่ยนรหัสพาสเวิร์ดบ่อยๆ และจับเวลาการใช้งาน

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
การเปลี่ยนรหัสผ่าน (Password) บ่อยๆ	ระบบควรจะเปลี่ยนรหัสพาสเวิร์ดให้อัตโนมัติทุกๆ 3-6 เดือนและทดสอบความปลอดภัยให้	มีการยกเลิกการใช้งานชั่วคราวหากผู้ใช้ไม่มีการใช้งานนานเกิน 1 เดือน และแจ้งเตือนผู้ดูแลระบบ
ด้านอุปกรณ์ (Hardware)		
อุปกรณ์และระบบปฏิบัติการ (Operating System) มีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	อุปกรณ์และระบบปฏิบัติการ (Operating System) ของกรมฯ จะต้องมีความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27000 และรองรับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ศทส. จะต้องมีการดำเนินการอบรมหรือได้รับวุฒิบัตรด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ (Operating System) ตามมาตรฐานสากล ISO/IEC 27000 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
การกำหนดใช้ตระกูลไมโครโปรเซสเซอร์	ควรใช้ตระกูล Intel หรือ AMD สำหรับเครื่องคอมพิวเตอร์แม่ข่าย/ลูกข่าย/โน้ตบุ๊ก	ศทส. ควรช่วยคัดเลือกตามสเปกที่กระทรวง ICT กำหนดและเลือกใช้ตระกูล Intel หรือ AMD
การทดแทนอุปกรณ์ที่อายุมาก	ต้องเตรียมงบประมาณเพื่อจัดหาเครื่องทดแทน	มีการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ทุกๆ 3-6 เดือน
การซ่อมบำรุงอุปกรณ์	ต้องเตรียมงบประมาณฉุกเฉิน	มีการจัดซื้ออะไหล่อุปกรณ์ที่เหมือนกันมาเก็บไว้
การนำอุปกรณ์ส่วนตัวมาใช้งานในองค์กร	อนุญาตให้นำมาใช้ได้ แต่ต้องมีการทดสอบด้านความปลอดภัย	มีซอฟต์แวร์ทดสอบด้านความปลอดภัย มีระบบล็อก (log) ตาม พ.ร.บ. คอมพิวเตอร์
การนำอุปกรณ์จากหน่วยงานอื่นๆ มาใช้งานในองค์กร	อนุญาตให้นำมาใช้ได้ แต่ต้องมีการทดสอบด้านความปลอดภัย	-----”-----
การติดตามและควบคุมการใช้	การนำอุปกรณ์ออกไปใช้งานนอกสถานที่ทุกครั้งต้องมีการทดสอบด้านความปลอดภัยเมื่อนำกลับมาใช้ภายใน	-----”-----

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
การควบคุมปริมาณอุปกรณ์	ควรมีการนับจำนวนและควบคุมจำนวนอุปกรณ์ที่เชื่อมต่อเครือข่ายอินเทอร์เน็ต	มีระบบนับจำนวนและควบคุมจำนวนอุปกรณ์ที่เชื่อมต่อเครือข่ายอินเทอร์เน็ตพร้อมๆ กัน มีการควบคุมบิตเรทของการเชื่อมต่อ
ด้านซอฟต์แวร์ (Software)		
ระบบสารสนเทศมีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ระบบสารสนเทศของกรมฯ จะต้องมีความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27000 และรองรับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ศทส. จะต้องมีการเจ้าหน้าที่ผ่านการอบรมหรือได้รับวุฒิบัตรด้านความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐานสากล ISO/IEC 27000 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
กำหนดเทคโนโลยีด้านซอฟต์แวร์ที่ชัดเจนในแต่ละด้าน	กำหนดเทคโนโลยีด้านซอฟต์แวร์ที่ชัดเจนในแต่ละด้าน เช่น ระบบปฏิบัติการ ระบบ DBMS GIS เป็นต้น เพื่อเอกภาพในการเรียนรู้ ฝึกอบรม และใช้งาน	ศทส. นักธรณี และนักภูมิสารสนเทศ ควรช่วยกันกำหนดเทคโนโลยีด้านซอฟต์แวร์ที่ชัดเจนในแต่ละด้าน เช่น ระบบปฏิบัติการ ระบบ DBMS GIS เป็นต้น เพื่อเอกภาพในการเรียนรู้ ฝึกอบรม และใช้งาน
การจัดหาระบบสารสนเทศใหม่	จะต้องปฏิบัติตามขั้นตอนการทดสอบระบบด้านความปลอดภัยก่อนใช้งาน	มีตารางจัดเก็บหมายเลขไอพีแอดเดรส มีการเฝ้าระวังพฤติกรรมในเครือข่าย
การบำรุงรักษาระบบสารสนเทศ	จะต้องมีการบำรุงรักษาทุกๆ 6 เดือน	มีระบบบันทึกการบำรุงรักษาในแต่ละครั้ง
การติดตั้งซอฟต์แวร์ลิขสิทธิ์	ควรมีการปรับเพิ่มจำนวนการใช้งาน	ระบบ Rollback การติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ การแพ็ทช์ระบบ การอัปเดตระบบ การปรับแต่งระบบเพื่อความปลอดภัย
การต่ออายุซอฟต์แวร์ลิขสิทธิ์บางประเภท	ควรจะต้องงบประมาณรองรับ มีการประเมินประสิทธิผลที่ได้ก่อนการต่ออายุ	การวิเคราะห์พฤติกรรมการใช้งานเครื่องคอมพิวเตอร์ การอัปเดตฐานข้อมูลไวรัส (Virus Signature) กับเครื่องที่ต่ออายุแล้ว
การติดตั้งซอฟต์แวร์ไม่มีลิขสิทธิ์	ควรมีการปรับลดจำนวนการใช้งาน	ส่งเสริมการใช้งานซอฟต์แวร์ที่เป็นโอเพนซอร์สมากขึ้น

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
การใช้ซอฟต์แวร์นอกเหนือจากงานที่ได้รับมอบหมาย	ควรมีการปรับลดจำนวนการใช้งานลง	ควรติดตั้งโปรแกรมเฝ้ามองการใช้งานเครื่องแต่ละเครื่อง ในบางส่วน/สำนัก
การใช้ข้อมูล/เว็บไซต์เพื่อความบันเทิง	ควรมีควบคุมให้สามารถใช้งานนอกเวลาราชการ	-----”-----
ด้านเครือข่าย (Network)		
ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	เครือข่ายทั้งมีสายและไร้สายของกรมฯ จะต้องมีความปลอดภัยตามมาตรฐานสากล ISO/IEC 27000 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ศทส. จะต้องมีการเจ้าหน้าที่ผ่านการอบรมหรือได้รับวุฒิบัตรด้านความปลอดภัยของเครือข่ายตามมาตรฐานสากล ISO/IEC 27000 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
เครือข่ายมีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	เครือข่ายทั้งมีสายและไร้สายของกรมฯ จะต้องมีความปลอดภัยตามมาตรฐานสากล ISO/IEC 27000 และรองรับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ศทส. จะต้องมีการเจ้าหน้าที่ผ่านการอบรมหรือได้รับวุฒิบัตรด้านความปลอดภัยของเครือข่ายตามมาตรฐานสากล ISO/IEC 27000 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
กำหนดเทคโนโลยีด้านเครือข่ายที่ชัดเจน	กำหนดเทคโนโลยีด้านเครือข่ายที่ชัดเจนในแต่ละด้าน เช่น ระบบปฏิบัติการของอุปกรณ์เครือข่าย เพื่อเอกภาพในการเรียนรู้ ฝึกอบรม และใช้งานด้านความมั่นคงปลอดภัย	ศทส. ควรร่วมมือกันกำหนดเทคโนโลยีด้านเครือข่ายที่ชัดเจนในแต่ละด้าน เช่น ระบบปฏิบัติการของอุปกรณ์เครือข่าย เพื่อเอกภาพในการเรียนรู้ ฝึกอบรม และใช้งานด้านความมั่นคงปลอดภัย
การเข้าถึงทางเครือข่ายจากภายนอกสู่ภายใน	จะต้องปิด/เปิดให้ใช้งานได้เพียงบาง Port ที่จำเป็นและบางช่วงเวลา	-----”-----

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
การเข้าถึงทางเครือข่ายจากภายในสู่ภายนอก	จะต้องปิด/เปิดให้ใช้งานได้เพียงบาง Port ที่จำเป็นและบางช่วงเวลา	การติดตั้งโปรแกรมไฟร์วอลล์ ระบบตรวจจับและป้องกันการบุกรุกทางเครือข่าย (Network Intrusion Detection/Protection System)
การเปิด/ปิดการใช้เครือข่ายในบางช่วงเวลา	จะต้องปิด/เปิดให้ใช้งานได้เพียงบาง Port ที่จำเป็นและบางช่วงเวลา	การปรับตั้งค่าให้เหมาะสมกับการใช้งานเครือข่าย การเฝ้าระวังพฤติกรรมที่ไม่เหมาะสมทางเครือข่าย
การเปิด/ปิดการใช้เครือข่ายในบางเว็บไซต์ในบางช่วงเวลา	จะต้องปิด/เปิดให้ใช้งานได้เพียงบางเว็บไซต์ที่จำเป็นและบางช่วงเวลา	การจับเวลาการใช้งานเครือข่าย การนับปริมาณการใช้เครือข่าย
การแชร์ไฟล์ผ่านระบบ P2P	จะต้องปิด/เปิดให้ใช้งานได้เพียงบางเว็บไซต์ที่จำเป็นและบางช่วงเวลา	-----”-----
การควบคุมการใช้งานเครือข่ายอินเทอร์เน็ตบนอุปกรณ์บางตัว	การเปิด/ปิดการใช้เครือข่ายสำหรับอุปกรณ์บางตัว ในบางช่วงเวลา	การลงทะเบียนการใช้งานอุปกรณ์ การตั้งค่าไอพีแอดเดรสให้อุปกรณ์อย่างเป็นระบบ
ด้านขั้นตอนการทำงาน (Procedure)		
ขั้นตอนปฏิบัติงานตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	กรมฯ จะต้องมีขั้นตอนการปฏิบัติงานตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ศทส จะต้องมีเจ้าหน้าที่ผ่านการอบรมพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
การวางแผนเมื่อเกิดภัยพิบัติ	ข้อมูลทั้งหมดของระบบสารสนเทศควรจะต้องมีการสำรองไว้ในที่ปลอดภัย	มีการจัดทำแผนการอย่างละเอียดและฝึกซ้อมการปฏิบัติงานเป็นระยะๆ เพื่อป้องกันความสับสน

ขั้นตอนการปฏิบัติงานความมั่นคงปลอดภัย	ระดับกรมฯ	แผนงานระดับกรมฯ และหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
ลำดับขั้นตอนการตัดสินใจในสถานการณ์ปกติและฉุกเฉิน	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ จะต้องมีความรู้และมีสิทธิ์ในการตัดสินใจในสถานการณ์ฉุกเฉินและปกติ	-----”-----
การตอบสนองต่อสถานการณ์ฉุกเฉิน	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบสั่งการให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ ดูแลระบบเพื่อตอบสนองต่อสถานการณ์	-----”-----
การกู้คืนระบบ	ระบบจะต้องสามารถกลับมาทำงานได้เหมือนปกติภายใน 24-48 ชั่วโมง เมื่อเหตุการณ์คลี่คลาย	-----”-----
ขั้นตอนการจัดหาอุปกรณ์เพิ่มเติม	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ จะต้องมอบหมายความรับผิดชอบให้กับหัวหน้ากลุ่มวิชาการและวางแผน และหัวหน้ากลุ่มคอมพิวเตอร์และระบบสื่อสาร	จัดทำขั้นตอนการดำเนินการที่ชัดเจน เริ่มต้นจากการจัดทำสเปกการจัดหา การติดตั้ง การทดสอบความปลอดภัย การบำรุงรักษา และการทดแทนเมื่อหมดอายุ

6.7 สรุปความแตกต่างระหว่างสถาปัตยกรรมใหม่และเก่า

ถึงแม้ระบบสารสนเทศในสถาปัตยกรรมเก่าส่วนใหญ่เป็นชนิดเว็บแอปพลิเคชัน แต่กรมายังขาดรายละเอียดในด้านพื้นฐานของระบบสารสนเทศ เช่น ด้านข้อมูล ด้านบุคลากร ด้านขั้นตอนการปฏิบัติการ เป็นต้น ตารางที่ 6.7.1 ได้สรุปความแตกต่างระหว่างสถาปัตยกรรมใหม่และเก่าในด้านต่างๆ ดังนี้

ตารางที่ 6.7.1 สรุปความแตกต่างระหว่างสถาปัตยกรรมใหม่และเก่า

ความแตกต่าง	สถาปัตยกรรมใหม่	สถาปัตยกรรมเก่า
ด้านข้อมูล (Data)		
มาตรฐานพิกัดตำแหน่ง มาตรฐานชนิดข้อมูลต่างๆ ระหว่างระบบสารสนเทศ	กำหนดแนวทางในการจัดทำขั้นตอน ปฏิบัติในด้านข้อมูล	ไม่มีหรือไม่ได้กำหนดใช้
การจัดทำฐานข้อมูลกลางของ กรมฯ	ริเริ่มและจัดทำให้เป็นมาตรฐาน การปฏิบัติงาน	มีการจัดเก็บข้อมูลที่ซ้ำซ้อน เนื่องจากไม่มีฐานข้อมูลกลาง
ด้านบุคลากร (Personnel)		
การบริหารจัดการและ ฐานข้อมูลบุคลากร/ผู้ใช้งาน	ใช้ฐานข้อมูลกลางเพียงระบบเดียว และเชื่อมโยงกับระบบยืนยันตัว บุคคลตาม พ.ร.บ. คอมพิวเตอร์ พ.ศ.2550	มีการจัดทำแยกและไม่ได้เชื่อมโยง กับระบบยืนยันตัวบุคคลตาม พ.ร.บ. คอมพิวเตอร์ พ.ศ.2550
การฝึกอบรมและการทดสอบ ด้านการใช้เทคโนโลยี สารสนเทศและการสื่อสาร	บรรจุอยู่ในแผนฯและต้องสอดคล้อง กับเทคโนโลยีในสถาปัตยกรรมใหม่	มีการใช้งานเทคโนโลยีที่ หลากหลายทำให้บุคลากรเรียนรู้ ได้ไม่เต็มที่
ด้านอุปกรณ์ (Hardware)		
มีความปลอดภัยตาม พระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การทดแทนอุปกรณ์ที่อายุมาก และการซ่อมบำรุงอุปกรณ์	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การควบคุมการใช้งานอุปกรณ์ ที่นำเข้ามาและออกจากกรมฯ	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การจัดหาอุปกรณ์ด้าน เทคโนโลยีสารสนเทศของกรมฯ	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
ด้านซอฟต์แวร์ (Software)		

ความแตกต่าง	สถาปัตยกรรมใหม่	สถาปัตยกรรมเก่า
มีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การจัดหาระบบสารสนเทศใหม่และการบำรุงรักษาระบบสารสนเทศ	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การติดตั้งซอฟต์แวร์ลิขสิทธิ์และต่ออายุซอฟต์แวร์ลิขสิทธิ์	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์เพื่อปฏิบัติงานและการใช้งานนอกเหนืองานที่ได้รับ	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
ด้านเครือข่าย (Network)		
ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	มีแต่การขาดการบังคับใช้งาน
มีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การควบคุมการใช้เครือข่ายเพื่อความปลอดภัย	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	มีแต่การขาดการบังคับใช้งาน
การเพิ่มความเร็วสายอินเทอร์เน็ตทั้งหมดของกรมฯ	เพื่อรองรับการใช้งานที่เพิ่มขึ้นและการใช้งานระบบวีดีโอคอนเฟอเรนซ์	ไม่มีหรือไม่ได้กำหนดใช้
การเพิ่มสายอินเทอร์เน็ตสำรองในแต่ละศูนย์เขต เพื่อเพิ่มความเชื่อมั่น	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	มีการจัดทำเองในบางศูนย์เขต
ด้านขั้นตอนการทำงาน (Procedure)		
มีความปลอดภัยตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	ได้บรรจุในแผนแม่บทฯ เพื่อร่างแนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้

ความแตกต่าง	สถาปัตยกรรมใหม่	สถาปัตยกรรมเก่า
การวางแผนเมื่อเกิดภัยพิบัติ และลำดับขั้นตอนการตัดสินใจ ในสถานการณ์ปกติและฉุกเฉิน	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้
การกู้คืนระบบ	ได้บรรจุในแผนแม่บทฯ เพื่อร่าง แนวทางให้ปฏิบัติตาม	ไม่มีหรือไม่ได้กำหนดใช้