ทิศทางและนโยบายเทคโนโลยีสารสนเทศของสภากาชาดไทย

นายบุญรักษ์ สรัคคานนท์

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

วันพฤหัสบดีที่ 4 กรกฎาคม 2562 เวลา 09:00 – 10:00 น.

โรงพยาบาลสมเด็จบรมราชเทวี ณ ศรีราชา

ทิศทางและนโยบายเทคโนโลยีสารสนเทศของสภากาชาดไทย

- ประวัติความเป็นมาและภารกิจของศูนย์เทคโนโลยีสารสนเทศ
- โครงสร้างการบริหาร
- การพัฒนาและการใช้งานระบบสารสนเทศของสภากาชาดไทยในปัจจุบัน
- บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ
- ทิศทางแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย
- นโยบายการดำเนินงานด้านเทคโนโลยีสารสนเทศของสภากาชาดไทย
- นโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศสภากาชาดไทย
- พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พรบ.คุ้มครองข้อมูลส่วนบุคคล

ประวัติความเป็นมา และภารกิจของศูนย์เทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศ สภากาชาดไทย ก่อตั้งขึ้นเมื่อวันที่ 1 ตุลาคม 2543 โดยเริ่มมีการใช้ระบบคอมพิวเตอร์และอินเทอร์เน็ตอย่างเป็นระบบมากขึ้น

ในช่วงปี 2540 ได้รับการสนับสนุนช่องทางออกสู่อินเทอร์เน็ตจากโครงการพัฒนาข้อมูลข่าวสารสภากาชาดไทยบนอินเทอร์เน็ตในเครือข่ายกาญจนาภิเษกตามพระราชดำริ สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี รวมทั้งการออกสู่อินเทอร์เน็ตผ่านทางคณะแพทยศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ต่อมาได้มีการพัฒนาเว็บไซต์ของสภากาชาดไทยและระบบสารสนเทศหลักในด้านงาน เงิน คน และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนงานตามภารกิจหลักของทุกหน่วยงานในสภากาชาดไทย

มีคณะกรรมการพัฒนานโยบายเทคโนโลยีสารสนเทศ สภากาชาดไทย ทำหน้าที่ กำหนดนโยบาย แนวทางการดำเนินงาน ทิศทางองค์กรด้าน ICT และภาพรวมในการพัฒนาระบบสารสนเทศให้กับสภากาชาดไทย ตั้งแต่ปี 2550 โดยได้รับการสนับสนุนจากผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ และหน่วยงานต่างๆ มาจนถึงปัจจุบัน

ภารกิจหลักของศูนย์เทคโนโลยีสารสนเทศ

ตามข้อบังคับของสภากาชาดไทย แก้ไขเพิ่มเติม พุทธศักราช 2549 หมวดที่ 7 กิจการของสภากาชาดไทย ข้อ 42 สัตต : มีหน้าที่

1 พัฒนาระบบเทคโนโลยีสารสนเทศของสภากาชาดไทย

2 เป็นศูนย์กลางในการเชื่อมโยงให้คำปรึกษา และ

3 ร่วมพัฒนาระบบเทคโนโลยีสารสนเทศของหน่วยงานอื่นๆ รวมทั้งมีหน้าที่

4 พัฒนาบุคลากรและผู้บริหารให้มีศักยภาพในการใช้เทคโนโลยีสารสนเทศเพื่อเพิ่มประสิทธิภาพ และประสิทธิผลในการดำเนินงาน และ

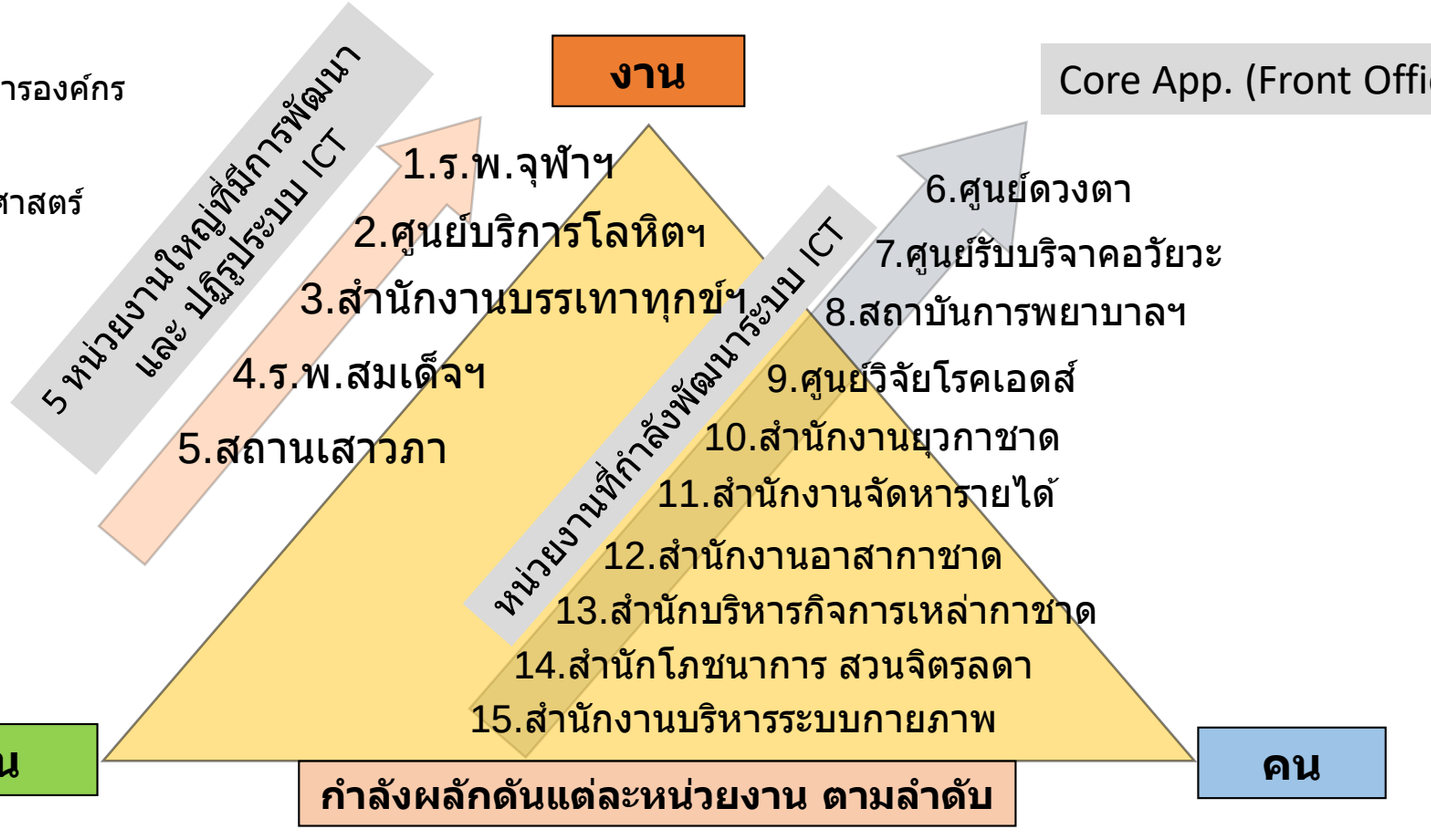
5 สามารถใช้เป็นสื่อประชาสัมพันธ์ได้ทั้งภายในและภายนอกรวมทั้งต่างประเทศ

ความก้าวหน้าด้าน ICT
ของ 25 หน่วยงานในสภากาชาดไทย

หน่วยงานที่ต้องพัฒนาระบบ ICT

16.สำนักงานบริหาร
- 16.1 สำนักสารนิเทศและสื่อสารองค์กร
- 16.2 สำนักวิเทศสัมพันธ์
- 16.3 สำนักนโยบายและยุทธศาสตร์

17. มูลนิธิสงเคราะห์เด็กฯ
18. สำนักงานจัดการทรัพย์สิน
19. สำนักงานกลาง
20. สำนักงานตรวจสอบ
21. ศูนย์เวชศาสตร์ฟื้นฟู
22. ศูนย์ฝึกอบรมปฐมพยาบาลฯ



Core App. (Back Office)

FMIS ระบบการเงิน งบประมาณ จัดซื้อ คลังพัสดุ บริจาคเงิน ครุภัณฑ์

HRMi ระบบบุคลากร ประเมินผล สมัครงาน ฝึกอบรม เงินเดือน สวัสดิการ

23.สำนักงานการคลัง

โครงสร้างพื้นฐาน ICT

24.สำนักงานบริการทรัพยากรบุคคล

ระบบคอมพิวเตอร์ Data Center / Cloud Service ซอฟต์แวร์ เน็ตเวิร์ก อีเมล์ เว็บไซต์ อินทราเน็ต eDOC.ระบบสารบรรณ คน IT

25.ศูนย์เทคโนโลยีสารสนเทศ

โครงสร้างการบริหาร

ปี 2550 แต่งตั้งคณะกรรมการพัฒนาเทคโนโลยีสารสนเทศสภากาชาดไทย

บทบาทหน้าที่ :

1. เสนอนโยบายข้อเสนอแนะ วิเคราะห์ แก้ไขปัญหาและประสานงานในการผลักดันระบบงานด้าน ICT ของสภากาชาดไทย
2. เสนอนโยบายและข้อเสนอแนะในการบริหารจัดการกำลังบุคลากรและงบประมาณด้าน ICT ที่เพียงพอต่อการพัฒนางานด้าน ICT ของสภากาชาดไทย
3. ติดตามและประเมินผลสัมฤทธิ์ของการพัฒนาระบบงานด้าน ICT เพื่อใช้ในการพัฒนาและปรับปรุงแนวทางการดำเนินงานด้าน ICT รวมทั้งแผนแม่บท ICT ในช่วงต่อไป
4. ดำเนินงานด้าน ICT ตามที่ได้รับมอบหมายจากสภากาชาดไทย

ปี 2560 แต่งตั้งคณะกรรมการบริหารศูนย์ฯ

บทบาทหน้าที่ :

1. กำหนดนโยบาย แผนยุทธศาสตร์และแนวทางการบริหารจัดการงานด้าน ICT ของศูนย์เทคโนโลยีสารสนเทศ สภากาชาดไทย
2. พิจารณา เสนอแนะ กลั่นกรอง และให้ความเห็นชอบแผนงาน/โครงการและงบประมาณรายจ่ายประจำปี ด้าน ICT ของศูนย์เทคโนโลยีสารสนเทศ สภากาชาดไทย
3. กำกับ ดูแล ติดตามประเมินผล แผนงาน / โครงการด้าน ICT ของศูนย์เทคโนโลยีสารสนเทศ สภากาชาดไทย ให้เป็นไปอย่างมีประสิทธิภาพ

การพัฒนาและการใช้งานระบบสารสนเทศของสภากาชาดไทยในปัจจุบัน

หน่วยงานเจ้าของ (Owner)	ชื่อระบบ	ปีที่เริ่มใช้งาน	จำนวนผู้ใช้งาน
โรงพยาบาลจุฬาลงกรณ์	โครงการพัฒนาระบบเทคโนโลยีสารสนเทศ HISใหม่	ปี 2558	4,000 User
โรงพยาบาลสมเด็จบรมราชเทวี ณ ศรีราชา	โครงการพัฒนาระบบเทคโนโลยีสารสนเทศ HIS	ปี 2547	2,000 User
ศูนย์บริการโลหิตแห่งชาติ	ระบบสารสนเทศงานบริการโลหิต (Hematos IIG)	9 ก.ค. 2556	1,000 User
	โครงการระบบสารสนเทศ Stem Cells (CeLIMS)	อยู่ระหว่างพัฒนา	ยังไม่เริ่มใช้งาน
สำนักงานการคลัง	โครงการพัฒนาระบบสารสนเทศการเงินสภากาชาดไทย (FMIS)	1 ต.ค. 2557	3,107 User
สถาบันการพยาบาลศรีสวรินทิรา	โครงการพัฒนาระบบบริหารจัดการบุคลากรของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย (สพศก.)	1 ก.พ. 2561	205 User
	โครงการพัฒนาระบบสารสนเทศการเงินของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย (FMIS สพศก.)	4 มิ.ย. 2561	205 User
	โครงการพัฒนาระบบฐานข้อมูลบริหารงานบริการการศึกษา และการบริหารงานและพัฒนาสมรรถนะบุคลากร	อยู่ระหว่างพัฒนา	ยังไม่เริ่มใช้งาน
สำนักงานจัดหารายได้	ระบบฐานข้อมูลผู้บริจาคเพื่อสนับสนุนงานหารายได้ (DMIS) version 1.0 & 1.5	1 ม.ค. 2561	40 User
	ระบบฐานข้อมูลผู้บริจาคเพื่อสนับสนุนงานหารายได้ (DMIS) version 2.0	กำลังจัดทำ TOR	ยังไม่เริ่มใช้งาน

การพัฒนาและการใช้งานระบบสารสนเทศของสภากาชาดไทยในปัจจุบัน

หน่วยงานเจ้าของ (Owner)	ชื่อระบบ	ปีที่เริ่มใช้งาน	จำนวนผู้ใช้งาน
ศูนย์เทคโนโลยีสารสนเทศ	ระบบสารบรรณอิเล็กทรอนิกส์(e-Doc)	ปี 2548	1,026 User
สำนักงานอาสากาชาด	โครงการพัฒนาระบบอาสาสมัครสภากาชาดไทย (VTRIS)	ปี 2557	1,482 User
ศูนย์ดวงตา	โครงการพัฒนาระบบฐานข้อมูลศูนย์ดวงตา (EYE Bank)	ส.ค. 2557	200 User
สำนักงานบรรเทาทุกข์ฯ	โครงการปรับปรุง และพัฒนาระบบฐานข้อมูลภัยพิบัติและระบบภูมิสารสนเทศ (GIS) ระยะที่ 2	1 เม.ย. 2562	1,023 User
สำนักโภชนาการสวนจิตรลดา	โครงการพัฒนาระบบสารสนเทศเพื่อการจัดเก็บเมนูพระกระยาหาร (Royal Menu Database System : RMDS)	อยู่ระหว่างพัฒนา	3 User
สำนักงานบริหารระบบกายภาพ	โครงการจัดจ้างทำฐานข้อมูลอาคารดิจิทัล (Building Information Modeling : BIM)	อยู่ระหว่างพัฒนา	ยังไม่เริ่มใช้งาน
สำนักงานบริหารทรัพยากรบุคคล	โครงการพัฒนาระบบสารสนเทศด้านทรัพยากรบุคคลของสภากาชาดไทย (HRMi)	อยู่ระหว่างพัฒนา	ยังไม่เริ่มใช้งาน
ศูนย์วิจัยโรคเอดส์	โครงการพัฒนาระบบสารสนเทศทางการแพทย์ HIS	ปี 2553	60 User
ศูนย์รับบริจาคอวัยวะ	โครงการพัฒนาระบบเทคโนโลยีสารสนเทศ สำหรับการบริการอวัยวะและเนื้อเยื่อ ศูนย์รับบริจาคอวัยวะสภากาชาดไทย (ODCs)	อยู่ระหว่างพัฒนา	30 โรงพยาบาลเครือข่าย (150User)

บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

1. งานด้านการสนับสนุนและพัฒนาระบบสารสนเทศ

1.1 การพัฒนาเว็บไซต์สภากาชาดไทย (https://www.redcross.or.th) และเว็บไซต์อินทราเน็ต (http://intranet.redcross.or.th/)

- ระบบ E-Service และมีระบบจดหมายอิเล็กทรอนิกส์ (E-mail Office 365)
- ระบบจองรถยนต์ ระบบจองห้องประชุม และระบบใบลา
- ระบบสารบรรณอิเล็กทรอนิกส์ (e-Doc)
- ได้รับความอนุเคราะห์จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) นำระบบบริหารการประชุมมาใช้ในการประชุมกรรมการเจ้าหน้าที่และกรรมการบริหาร
- ให้บริการ Web Hosting

1.2 สนับสนุนการพัฒนาระบบสารสนเทศการเงินสภากาชาดไทย (FMIS) ตั้งแต่ปี 2557 จนถึงปัจจุบัน

- จัดการบทบาทและสิทธิ์ผู้ใช้งานระบบ FMIS
- จัดการรหัสวัสดุและครุภัณฑ์ทางการแพทย์
- สนับสนุนการเช่าเครื่องคอมพิวเตอร์ในการใช้งานระบบ FMIS จำนวน 1,040 เครื่อง
- สนับสนุน DR-Site
- สนับสนุนการย้ายระบบขึ้นคลาวด์
- สนับสนุนการจัดทำแผน BCP ระบบ FMIS

บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

1. งานด้านการสนับสนุนและพัฒนาระบบสารสนเทศ

1.3 สภากาชาดไทยได้ลงนาม MOU กับกรมการปกครองในการเชื่อมโยงข้อมูลทะเบียนราษฎร์
- แบบ Batch
- แบบ e-Mail
- แบบ Online
- Smart Card

1.4 สนับสนุนซอฟต์แวร์ (Software) เพื่อสนับสนุนการดำเนินงานตามภารกิจของสภากาชาดไทย ในการดำเนินการจัดซื้อและติดตั้งซอฟท์แวร์สำเร็จรูปถูกลิขสิทธิ์สำหรับการปฏิบัติงานให้แก่หน่วยงานที่ร้องขอ เช่น Windows, Adobe Acrobat, Microsoft Office เป็นต้น รวมถึงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่ติดตั้งสำหรับเครื่องคอมพิวเตอร์ของหน่วยงานในสภากาชาดไทย เพื่อป้องกัน และลดความเสี่ยงจากภัยคุกคามต่างๆ

1.5 ดำเนินการตรวจสอบช่องโหว่เว็บไซต์หน่วยงานในสภากาชาดไทย ตั้งแต่ปี 2561 จนถึงปัจจุบัน และในปี 2562 ได้รับความอนุเคราะห์จากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์มาดำเนินการตรวจสอบช่องโหว่เว็บไซต์หน่วยงานในสภากาชาดไทยที่เข้าร่วมโครงการฯ

บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

2. งานให้บริการด้านระบบเครือข่ายและอินเทอร์เน็ต

2.1 บริการการใช้งานระบบอินเทอร์เน็ตภายในสภากาชาดไทยทั้งส่วนกลางและส่วนภูมิภาค

ศูนย์เทคโนโลยีสารสนเทศมีหน้าที่ดูแลระบบเครือข่าย Internet ตั้งแต่ปี 2537 โดยได้รับบริจาคเครือข่ายกาญจนาภิเษก ขนาดความเร็ว 64 kbps พร้อมระบบโทรศัพท์ 16 คู่สาย จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) และได้เพิ่มขนาดความเร็วและขยายการให้บริการมาโดยตลอด ปัจจุบันขนาดความเร็ว

วงจรที่ 1 ขนาด 1 Gbps (UNINET) จำนวน 2 เส้นทาง ได้แก่ สภากาชาดไทยและมหาวิทยาลัยเกษตรศาสตร์ และ

วงจรที่ 2 ขนาด 1/300 Gbps (3BB) จำนวน 2 เส้นทาง ได้แก่ สภากาชาดไทยและมหาวิทยาลัยเกษตรศาสตร์

2.2 พัฒนา ดูแล บำรุงรักษา และให้บริการระบบเครือข่ายแก่หน่วยงานในสภากาชาดไทย การเชื่อมโยงเครือข่ายไปยังหน่วยงานส่วนภูมิภาคด้วย MPLS (Multiprotocol Label Switching)

ศูนย์เทคโนโลยีสารสนเทศได้เชื่อมโยงเครือข่ายด้วยเทคโนโลยี Multiprotocol Label Switching จากสภากาชาดไทยส่วนกลางไปยังส่วนภูมิภาคทั่วประเทศ เพื่อใช้งานระบบภายในต่างๆ เช่น Intranet, ระบบสารบัญอิเล็กทรอนิกส์ e-Doc , ระบบสารสนเทศการเงินสภากาชาดไทย (FMIS) เป็นต้น ปัจจุบัน จำนวน 33 แห่ง

2.3 พัฒนา ดูแล บำรุงรักษาศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) และศูนย์สำรองข้อมูลฉุกเฉิน (Disaster Recovery Site) ศูนย์ข้อมูลคอมพิวเตอร์ หรือห้อง Data Centre อาคารเทิดพระเกียรติพระญาณสังวร ปัจจุบันมีจำนวน 14 ตู้ Rack เพื่อรองรับการใช้งานให้หน่วยงานของสภากาชาดไทยได้มากขึ้น

2.4 การดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย พ.ศ.2561 ของศูนย์เทคโนโลยีสารสนเทศ ได้ดำเนินการแต่งตั้งคณะกรรมการดำเนินการในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของสภากาชาดไทย โดยมีหน้าที่ผลักดันระเบียบสภากาชาดไทย ด้านความปลอดภัยของการใช้งานระบบคอมพิวเตอร์และสารสนเทศ ซึ่งได้ประกาศใช้ครั้งแรกในปี 2552 รวมถึงได้จัดการอบรมเพื่อสร้างความรู้ความเข้าใจ สร้างความตระหนักด้านความมั่นคงปลอดภัย ของสารสนเทศทั้งระดับเจ้าหน้าที่และระดับผู้บริหารอย่างต่อเนื่อง ตัวอย่างเช่น โครงการอบรมและประชาสัมพันธ์แนวทางการใช้งานระเบียบด้านความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศ, การอบรม พ.ร.บ. ว่าด้วยการกระทำผิดในการใช้ระบบคอมพิวเตอร์, การอบรม Cloud Computing Awareness, การอบรมนโยบาย แนวปฏิบัติ เพื่อการรักษาความมั่นคงปลอดภัย (IT Policy)และแต่งตั้งคณะกรรมการบริหารนโยบายตรวจสอบและประเมินผลการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของสภากาชาดไทย

บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

2.5 จัดหา บริการ และสนับสนุนอุปกรณ์ระบบคอมพิวเตอร์ (Hardware) ให้หน่วยงานต่างๆ ของสภากาชาดไทย เพื่อให้เกิดความคุ้มค่าสูงสุด ง่ายต่อการบริหารจัดการ และเพิ่มประสิทธิภาพในการบำรุงรักษา ศูนย์เทคโนโลยีสารสนเทศจึงจัดหาเครื่องคอมพิวเตอร์ในรูปแบบการเช่าเพื่อสนับสนุนการดำเนินงานของหน่วยงานต่างๆ ทั้งเครื่องคอมพิวเตอร์แบบประมวลผลทั่วไป PC All in one และเครื่องคอมพิวเตอร์พกพาแบบประมวลผลทั่วไป (Notebook)

2.6 บริการ และให้คำปรึกษาด้าน ICT กับหน่วยงานในสภากาชาดไทย (E-Service) มีการให้บริการแจ้งซ่อมบำรุงคอมพิวเตอร์ผ่านบริการแจ้งซ่อมบนเว็บไซต์ E-Service (eservice.redcross.or.th) และระบบ FMIS ผ่านเว็บ Service FMIS LOG (fmislog.redcross.or.th)

2.7 ดูแลและให้บริการจดหมายอิเล็กทรอนิกส์สภากาชาดไทย (E-Mail : @redcross.or.th) ศูนย์เทคโนโลยีสารสนเทศ ได้รับบริจาคระบบ Mail บน Office 365 on Cloud จากบริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด ให้แก่สภากาชาดไทย ตั้งแต่ปี 2557 ซึ่งสามารถรองรับจำนวนผู้ใช้งานได้ถึง 3,000 Accounts

2.8 จัดหาโปรแกรมระบบป้องกันไวรัสคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศได้จัดหา Hardware และ Software ในการบริหารจัดการไวรัสคอมพิวเตอร์ ตั้งแต่ปี 2545 และได้พัฒนาอย่างต่อเนื่องจนถึงปัจจุบัน โดยใช้ Trend Micro ซึ่งมีระบบบริหารจัดการและระบบวิเคราะห์การป้องกันไวรัสที่มีประสิทธิภาพ และรองรับผู้ใช้งานมากกว่า 1,500 License

บทบาทและความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ

2.9 ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (เครื่องแม่ข่ายและเครื่องลูกข่าย) ดำเนินการจัดหาระบบ Web Filtering และ IPS (Intrusion Protection System) และ IDS (Intrution Detection System) โดยได้เข้าร่วมโครงการ Government Threat Monitoring System (GTM) เป็นระบบที่วิเคราะห์และป้องกันการโจมตีโดยอาศัยวิธีการวิเคราะห์บันทึก (log) และความผิดปกติ (anomaly) ของระบบที่ใช้ในองค์กรรัฐ และ Next Generation Firewall

2.10 การจัดอบรมด้าน ICT ให้บุคลากรสภากาชาดไทย

- 2.10.1 อบรม "ก้าวหน้าการประยุกต์ใช้ Social Media เพื่อการสื่อสารยุคใหม่ของสภากาชาดไทย" แก่เจ้าหน้าที่สภากาชาดไทย ครั้งที่ 1 และ 2
- 2.10.2 อบรมเรื่อง “พร้อมเพย์ การเงินยุคใหม่ คนไทยยุคดิจิตอล” ระดับผู้บริหาร และบุคลากรทั่วไปของสภากาชาดไทย
- 2.10.3 อบรมหลักสูตรสร้างสรรค์สื่อภาพแทนข้อมูล Infographics แบบมืออาชีพโดยใช้ Microsoft PowerPoint
- 2.10.4 บรรยายชี้แจงเรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย พ.ศ.2561” ระดับผู้บริหารและระดับเจ้าหน้าที่
- 2.10.5 อบรมเรื่อง “สภากาชาดไทยยุคไทยแลนด์ 4.0”
- 2.10.6 ฝึกอบรมและทดสอบระดับความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

ประชุมกรรมการเจ้าหน้าที่ 25 มกราคม 2555

2.10.7 บรรยายเรื่อง “บล็อกเชน (Blockchain) และบิทคอยน์ (Bitcoin) กับงานของสภากาชาดไทย”

2.10.8 บรรยาย “การเตรียมความพร้อมรับมือ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กับงานสภากาชาดไทย”

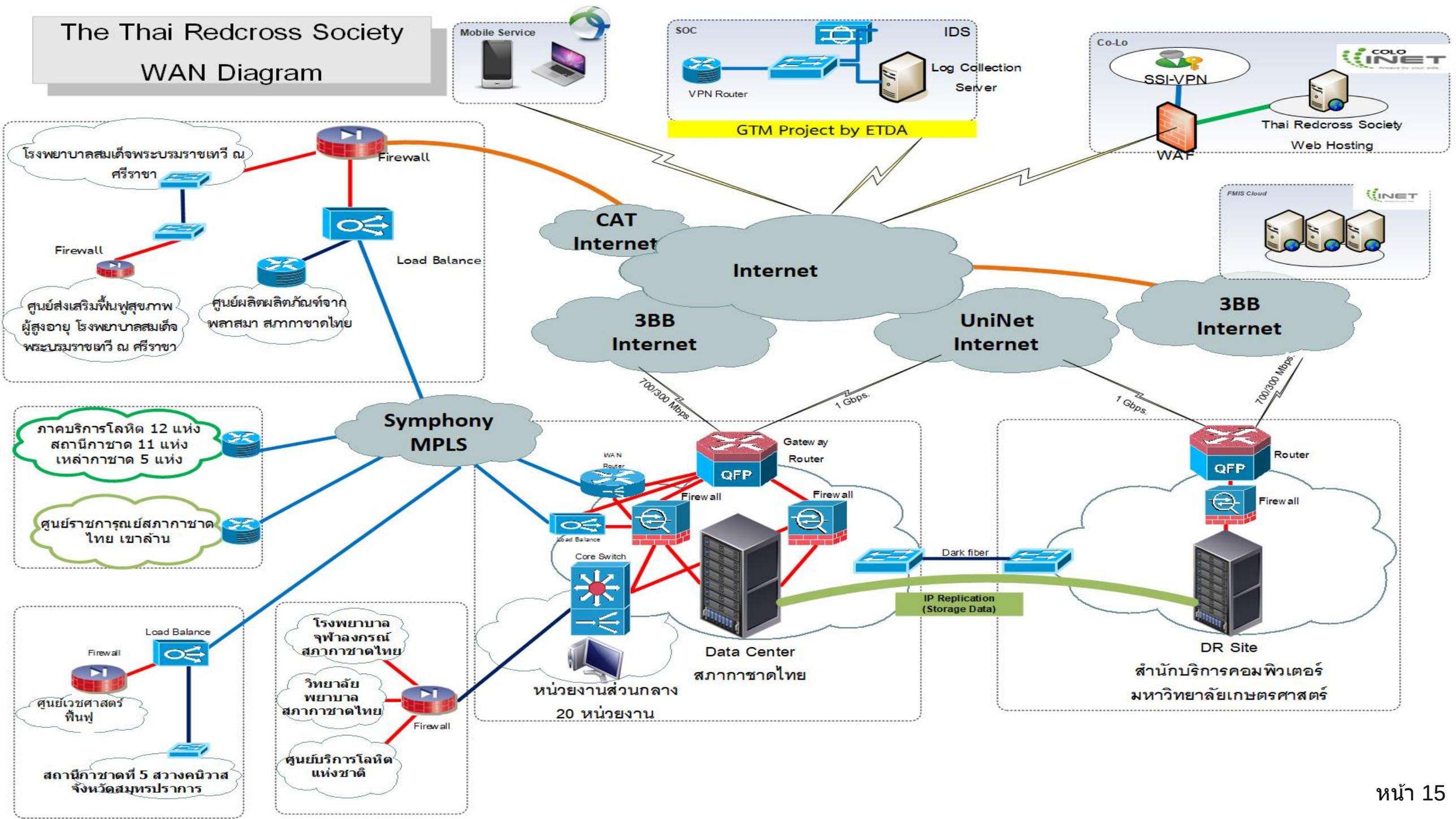
2.10.9 บรรยาย "การประยุกต์ใช้เทคโนโลยีดิจิทัล IoT และ Cloud computing กับงานภารกิจของสภากาชาดไทย" รอบผู้บริหารและบุคลากรทั่วไปของสภากาชาดไทย

3. งานด้านอื่นๆ

3.1 จัดซื้ออุปกรณ์ระบบคอมพิวเตอร์เพื่อรองรับและยกระดับกระบวนการจัดประชุมให้ก้าวทันเทคโนโลยียุคปัจจุบันฯ เป็นโครงการตามนโยบายของท่านเลขาฯ ในการลดใช้กระดาษที่เป็นเอกสารการประชุมของผู้บริหารโดยศูนย์ฯ ได้นำระบบบริหารการประชุม (E-Meeting) ซึ่งได้รับความอนุเคราะห์จาก NECTEC เข้ามาใช้ในการประชุมผู้บริหาร รวมถึงจัดซื้อเครื่อง iPad2 เพื่อรองรับการใช้งานระบบดังกล่าวแก่ผู้บริหารสภากาชาดไทย โดยที่ผ่านมาได้ทดลองการประชุมโดยใช้เครื่อง iPad2 และระบบบริหารการประชุม (E-Meeting) ในการประชุมกรรมการเจ้าหน้าที่ และกรรมการบริหารแล้ว

ประชุมกรรมการบริหาร 9 กุมภาพันธ์ 2555

The Thai Redcross Society
WAN Diagram



ทิศทางแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย พ.ศ.2552-2555 (ฉบับที่ 1) ประกาศใช้ ณ วันที่ 5 สิงหาคม 2552 และขยายแผนแม่บท จำนวน 2 ปี คือ ปี 2556-2557 ประกอบไปด้วย 5 ยุทธศาสตร์

ยุทธศาสตร์ที่ 1 พัฒนาระบบฐานข้อมูลงานบริการด้าน ICT

ยุทธศาสตร์ที่ 2 ยกระดับกระบวนการทำงานในทุกระบบงานและทุกหน่วยงานในสภากาชาดไทย

ยุทธศาสตร์ที่ 3 ปรับปรุงระบบเครือข่ายเน็ตเวิร์ค อุปกรณ์ระบบคอมพิวเตอร์และความมั่นคงปลอดภัยของระบบสารสนเทศทั้งสภากาชาดไทย

ยุทธศาสตร์ที่ 4 จัดหาอุปกรณ์และซ่อมบำรุงระบบคอมพิวเตอร์

ยุทธศาสตร์ที่ 5 พัฒนาบุคลากรของสภากาชาดไทยให้มีทักษะความรู้และมีศักยภาพต่อการทำงานรวมทั้งมีการจัดการความรู้พื้นฐานด้าน ICT ในการช่วยเหลือประชาชน

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย พ.ศ.2558-2560 (ฉบับที่ 2) ประกาศใช้ ณ วันที่ 19 มิถุนายน 2557 และขยายแผนแม่บท จำนวน 3 ปี คือ ปี 2561-2563 โดยตามมติ IT Steering ครั้งที่ 52 เมื่อวันที่ 17 พฤศจิกายน 2560 ประกาศใช้แผนแม่บทฯ 2561-2563 (ฉบับขยาย) ตั้งแต่ตุลาคม 2561 – กันยายน 2563 ประกอบไปด้วย 5 ยุทธศาสตร์ ดังนี้

ยุทธศาสตร์ที่ 1 การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อส่งเสริมและพัฒนาคุณภาพชีวิตของประชาชน

ยุทธศาสตร์ที่ 2 การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อการบริหารจัดการภายใน

ยุทธศาสตร์ที่ 3 การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อการทำงานร่วมกันระหว่างหน่วยงาน

ยุทธศาสตร์ที่ 4 การพัฒนาบุคลากรให้มีความพร้อมในการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

ยุทธศาสตร์ที่ 5 พัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อบริการหน่วยงานอย่างทั่วถึง

ทิศทางแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย

ร่างแผนแม่บทฯ พ.ศ.2564-2566

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย พ.ศ.2564-2566 (ฉบับที่ 3) ผ่านความเห็นชอบจากคณะกรรมการพัฒนานโยบายเทคโนโลยีสารสนเทศ ครั้งที่ 58 เมื่อวันที่ 24 พฤษภาคม 2562 รอนำเสนอเข้ากรรมการสภากาชาดไทย ในเดือนกันยายน 2562 โดยจะมีการประกาศใช้แผนแม่บทฯ ตั้งแต่ตุลาคม 2563 –กันยายน 2566 ประกอบไปด้วย 5 ยุทธศาสตร์ ดังนี้

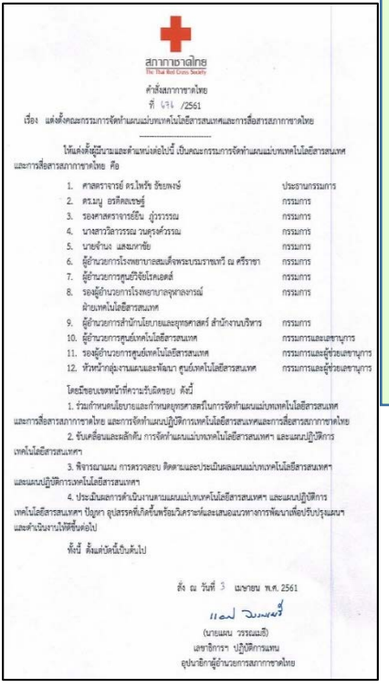
ยุทธศาสตร์ที่ 1 การนำเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) มาใช้สนับสนุนพันธกิจของสภากาชาดไทยอย่างมีประสิทธิผล

ยุทธศาสตร์ที่ 2 การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อการบริหารจัดการภายใน

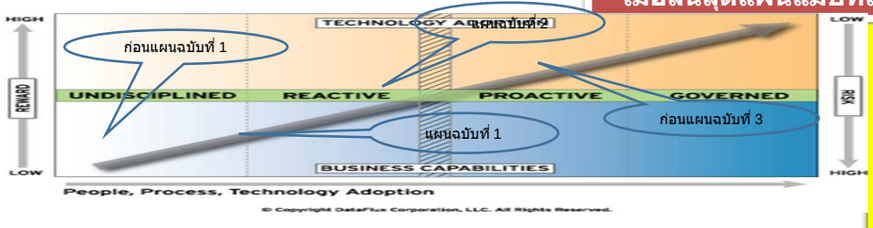
ยุทธศาสตร์ที่ 3 การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อบรูณาการการทำงานร่วมกันระหว่างหน่วยงาน

ยุทธศาสตร์ที่ 4 การพัฒนาบุคลากรให้มีความพร้อมในการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

ยุทธศาสตร์ที่ 5 พัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อบริการหน่วยงานอย่างทั่วถึง เสถียรและมั่นคงปลอดภัย



แต่งตั้งคณะกรรมการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย พ.ศ.2564-2566 (ฉบับที่ 3) คำสั่งสภากาชาดไทย ที่ 676/2561



เมื่อสิ้นสุดแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย

การประเมินวุฒิภาวะด้านข้อมูลองค์กรหลังแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย พ.ศ.2561-2563 (ส่วนต่อขยาย) ขั้นที่ 3 ขั้นมีมาตรการเชิงรุก (Proactive) ผู้บริหารส่วนใหญ่เริ่มเข้าใจความสำคัญของข้อมูลที่มีคุณภาพ และเข้ามีส่วนร่วม และสนับสนุนในการจัดทำระบบข้อมูลที่มีคุณภาพ

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารสภากาชาดไทย

ยุทธศาสตร์	กลยุทธ์	มาตรการ
1.การนำเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้สนับสนุนพันธกิจของสภากาชาดไทยอย่างมีประสิทธิผล	3	6
2.การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการบริหารจัดการภายใน	5	12
3.การประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการบูรณาการการทำงานร่วมกันระหว่างหน่วยงาน	4	10
4.การพัฒนาบุคลากรให้มีความพร้อมในการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสาร	3	6
5.การพัฒนาโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อบริการหน่วยงานอย่างทั่วถึง เสถียรและมั่นคงปลอดภัย	4	10
รวม	**19**	**44**

นโยบายการดำเนินงานด้านเทคโนโลยีสารสนเทศของสภากาชาดไทย

- นโยบายการให้คำปรึกษา การพัฒนาระบบสารสนเทศ และสนับสนุนการใช้งานระบบสารสนเทศอย่างเป็นมาตรฐาน (Core Application Support & Service)
- นโยบายการแลกเปลี่ยนข้อมูลและการเชื่อมต่อระบบงาน (Data Interchange & Application Integration)
- นโยบายการให้บริการเครื่องแม่ข่าย บริการเครือข่ายการติดต่อสื่อสารและบริการคลาวด์ (Infrastructure Support & Service)
- นโยบายการบริหารบุคคลากรไอที สภากาชาดไทย
  - IT Skill Standard System (ITSS) ระบบการประเมินความสามารถ ทักษะความชำนาญ เพื่อการพัฒนาบุคลากรด้าน IT อย่างเป็นระบบและมีมาตรฐาน
- นโยบายการจัดทำงบประมาณ และบริหารค่าใช้จ่ายด้าน IT
- นโยบายการจัดหาเครื่องคอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ไอที และการบำรุงรักษา (IT Device Support Service Procurement & MA Policy)

คุณลักษณะของเครื่องคอมพิวเตอร์ (ซื้อและเช่า)	Specification	PC All in One แบบประมวลผลทั่วไป	NB แบบประมวลผลทั่วไป	NB แบบประมวลผลสูง
	ราคา	32,000 บาท (รวม VAT7%)	30,000 บาท (รวม VAT7%)	47,000 บาท (รวม VAT7%)

IT Skill Standard System (ITSS)

- ITSS คือระบบการประเมินความสามารถ ทักษะความชำนาญ เพื่อการพัฒนาบุคลากรด้าน IT อย่างเป็นระบบ มีมาตรฐาน และเป็นรูปธรรม
- หน่วยงาน IPA ของญี่ปุ่นได้พัฒนาระบบ ITSS ขึ้น และสนับสนุนให้ผู้ประกอบการด้านซอฟต์แวร์ของญี่ปุ่นนำระบบนี้มาใช้ในการประเมินความสามารถและพัฒนาบุคลากรด้าน IT มาเป็นเวลานานอย่างต่อเนื่อง
- ในปี 2013 IPA ได้แนะนำให้ ATCI รู้จักและนำระบบ ITSS มาใช้ในองค์กรของผู้ประกอบการด้าน IT ของไทย โดยจัด Seminar และ Workshop เพื่อให้ความรู้และความเข้าใจในการนำระบบ ITSS มาใช้ในองค์กร
- IPA ได้คัดเลือกบริษัทไทยที่สนใจมาเป็นบริษัทนำร่อง (Pilot Company) เพื่อทดลองนำระบบ ITSS เข้าไปใช้ โดยเฉพาะกับองค์กรที่มีบุคคลากรด้าน Professional Service เป็นส่วนใหญ่ ซึ่งในระหว่างปี 2014 และ 2015 มีบริษัทที่สมัครเข้าร่วมเป็น Pilot Company รวม 8 บริษัท

IT Skill Standard System (ITSS)

ITSS Adoption Process

- เริ่มต้นจากการทำ Adoption Plan
- วางแผน Career Path, Job Category และ Job Level ของทั้งองค์กร
- กำหนดมาตรฐาน KPI และ Skill Proficiency ของแต่ละ Job
- ทำการประเมิน KPI และ Skill Proficiency ของพนักงานแต่ละคนเพื่อเปรียบเทียบกับมาตรฐานที่กำหนดไว้
- และจัดทำ Training Roadmap

KPI คือความสามารถและประสบการณ์ที่จะทำงานแต่ละ Job ประกอบด้วย

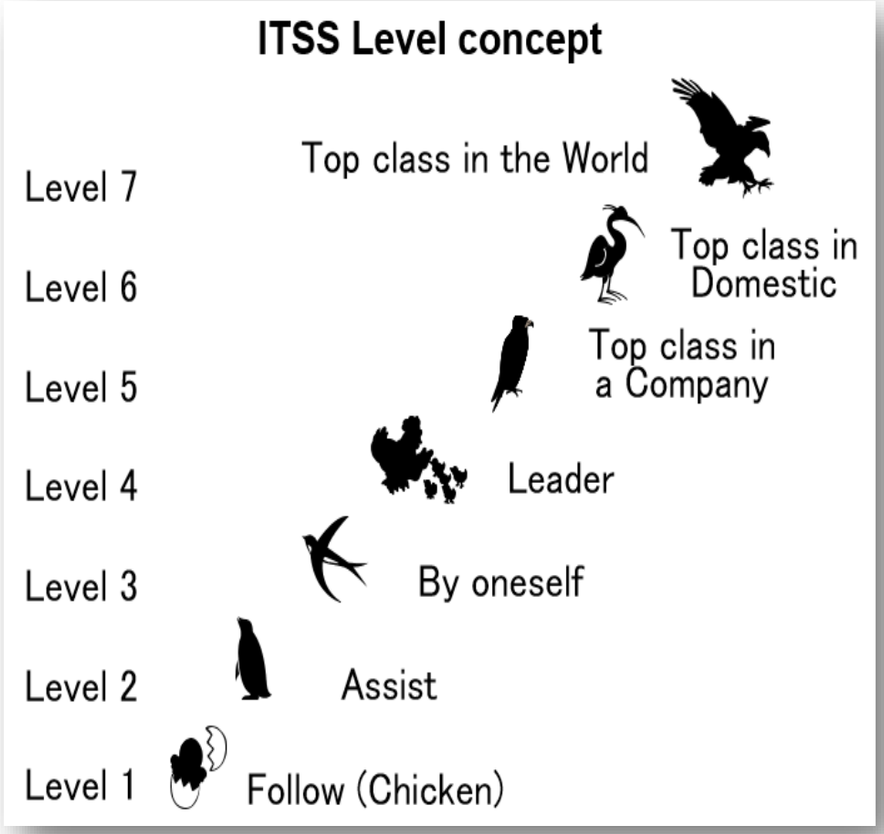
Business Contribution (หน้าที่รับผิดชอบ - responsibility, ความซับซ้อนของงาน - complexity, ขนาดของโครงการ - project size)

Professional Contribution (สิ่งที่ชำนาญเป็นพิเศษ - high specialty, การสืบทอดทักษะความรู้ความชำนาญ - expertise succession, การฝึกสอน coaching)

Skill Proficiency คือทักษะความชำนาญที่จะสามารถทำงานในแต่ละ Job ได้ ตัวอย่างเช่น personal skill, technology skill, methodology skill, project management skill, business & industry skill.

ตัวอย่าง Career Framework ขององค์กรซอฟต์แวร์ขนาดเล็ก

Job Categories	Software Technology		Software Project			Consulting	
Specialty Fields	Development	Product Support	QA/Tester	BA/SA	Project Manager	Product Consult	Business Consult
Level 7 Top Management							
Level 6 Professional							
Level 5 Expert							
Level 4 Leader							
Level 3 Sub-Leader							
Level 2 Assistant							
Level 1 Entry							



ตัวอย่าง Skill Proficiency

Personal	Leadership
	Communication
	Negotiation
	Customer Interaction (client mgmt.)
	Commitment
Technology	based on TRC Software
	Related Technology
Methodology	SDLC (Software Development Life Cycle)
	STLC (Software Testing Life Cycle)
	Software Quality Process
	ISO Quality Management
Project Mgmt	Project Approach
	Project Estimation, Project Planning
	Project Execution
	Project Monitor & control
Business/Industry	Financial Services Industry
	Enterprises
	Manufacturing

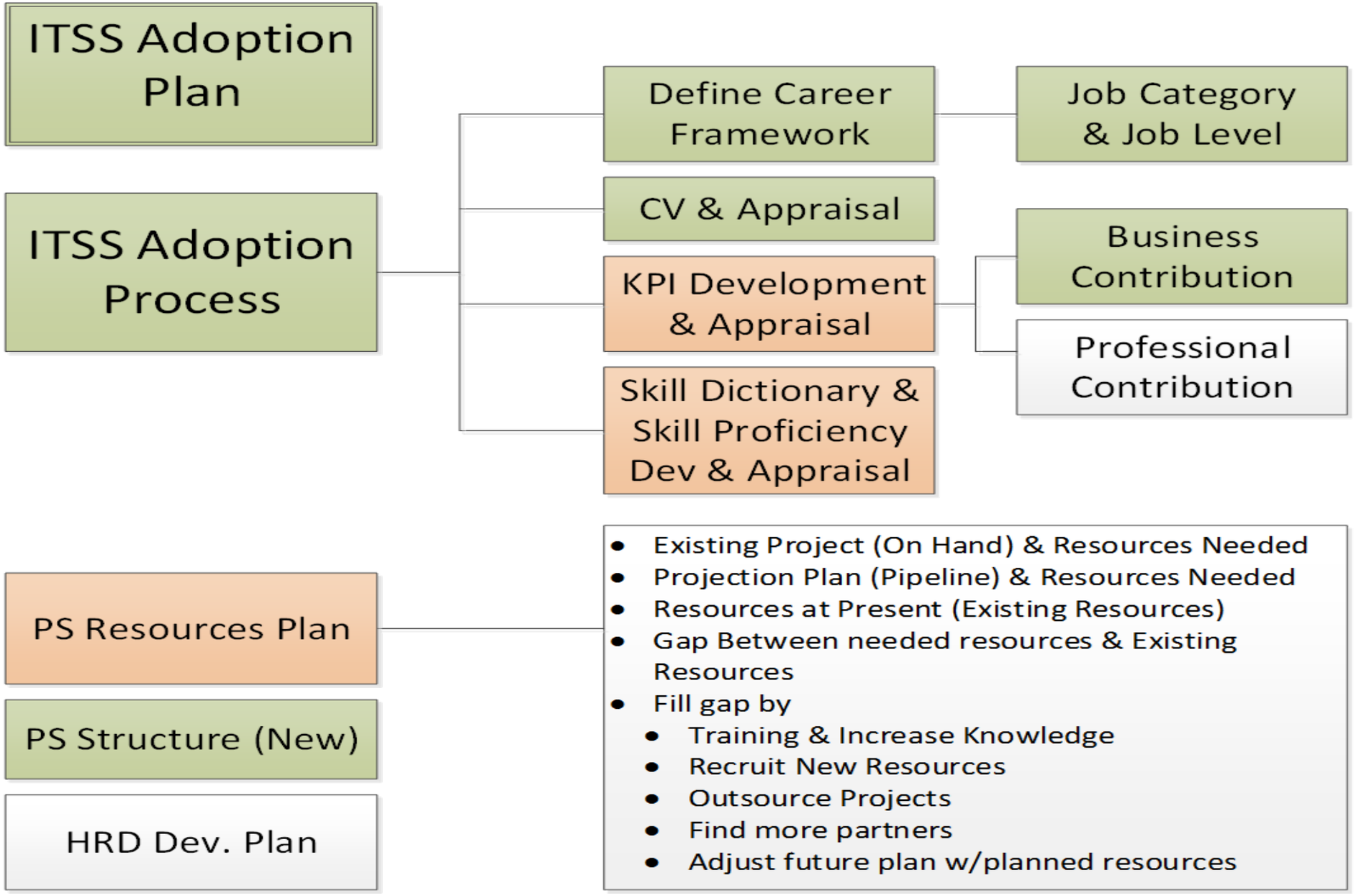
R1 มีความรู้ แต่ไม่เคยทำ

R2 พอทำได้แต่ต้องมีคนช่วย

R3 ทำได้เอง ไม่ต้องมีคนช่วย

R4 มีความรู้ ทำได้เอง และสามารถสอนผู้อื่นได้

ITSS & HR Plan


ITSS Adoption Plan
ITSS Adoption Process
Define Career Framework
Job Category & Job Level
CV & Appraisal
KPI Development & Appraisal
Business Contribution
Professional Contribution
Skill Dictionary & Skill Proficiency Dev & Appraisal
PS Resources Plan
PS Structure (New)
HRD Dev. Plan
Existing Project (On Hand) & Resources Needed
Projection Plan (Pipeline) & Resources Needed
Resources at Present (Existing Resources)
Gap Between needed resources & Existing Resources
Fill gap by
Training & Increase Knowledge
Recruit New Resources
Outsource Projects
Find more partners
Adjust future plan w/planned resources

องค์ประกอบของนโยบาย

ส่วนที่ 1 นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ 2 นโยบายการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

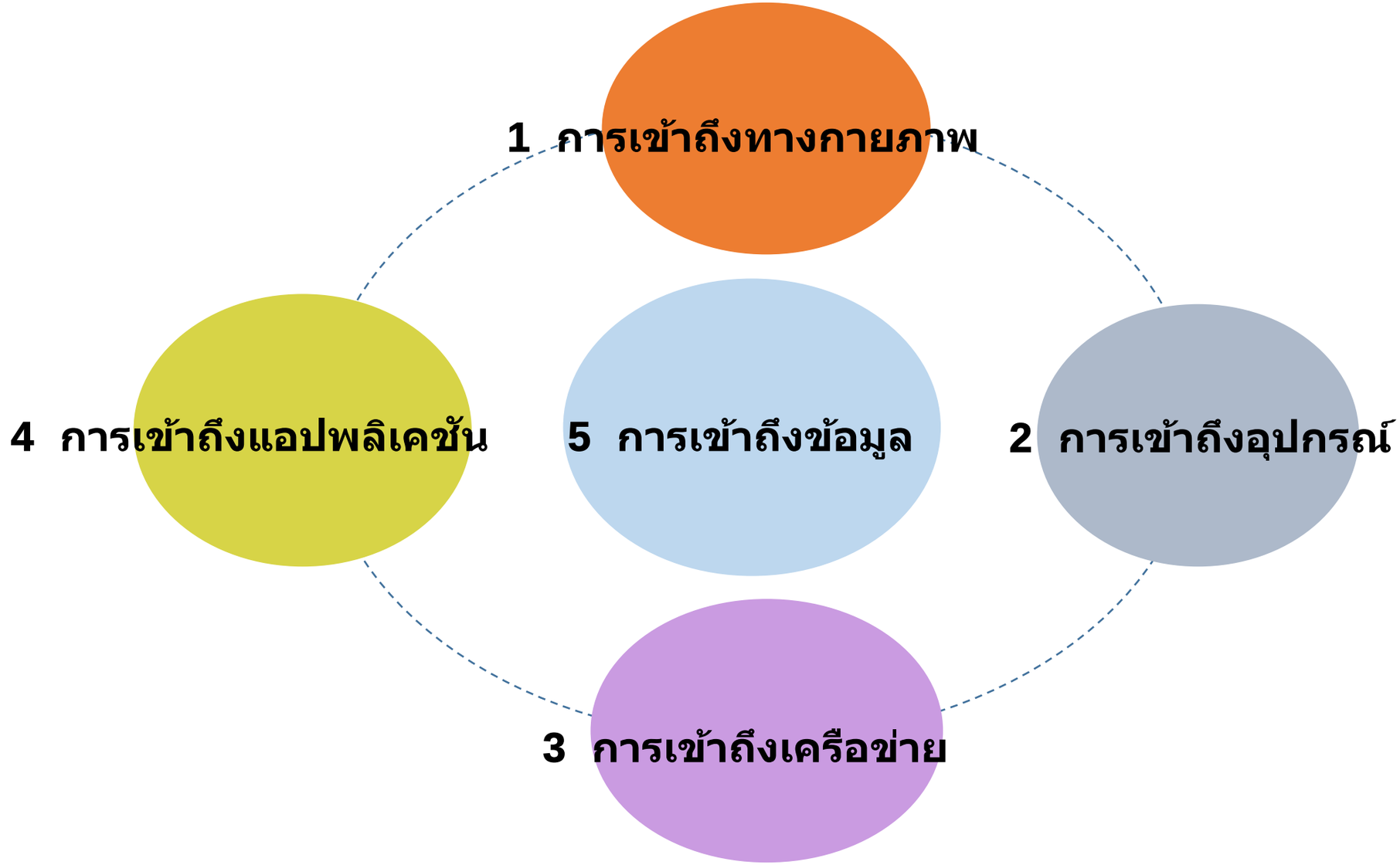
ส่วนที่ 4 นโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยด้านสารสนเทศ

ส่วนที่ 5 นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนที่ 6 นโยบายคุ้มครองข้อมูลส่วนบุคคล

นโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศสภากาชาดไทย

ส่วนที่ 1 นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ



ส่วนที่ 2 นโยบายการจัดทำระบบสำรองสารสนเทศ

แนวปฏิบัติ

- ระบบสำรอง (Disaster Recovery Site : DR Site)
- การสำรองข้อมูล (Data Backup)
- การกู้คืนข้อมูล (Data Recovery)
- การทดสอบสภาพพร้อมใช้งาน

ส่วนที่ 3 นโยบายการตรวจสอบ และประเมินความเสี่ยงสารสนเทศ

1. การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกอย่างน้อยปีละ 1 ครั้ง ตามที่ได้ดำเนินการแต่งตั้งเป็นที่เรียบร้อยแล้ว เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศโดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

1. จัดลำดับความสำคัญของความเสี่ยง
2. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
3. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
4. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
5. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
6. มีมาตรการในการตรวจประเมินระบบสารสนเทศต่างๆ (โดยจัดประชุมเพื่อชี้แจ้งอีกครั้ง)

ส่วนที่ 3 นโยบายการตรวจสอบ และประเมินความเสี่ยงสารสนเทศ

2. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

การติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศสามารถแยกเป็นภัยต่างๆ ได้ 4 ประเภท ดังนี้

ประเภทที่ 1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ประเภทที่ 2 ภัยที่เกิดจากซอฟต์แวร์ ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ 3 ภัยจากไฟไหม้หรือระบบไฟฟ้าจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ

ประเภทที่ 4 ภัยที่เกิดจากภัยธรรมชาติเช่นจาก ลมพายุ (วาตภัย) น้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 4 นโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยด้านสารสนเทศ

1. จัดให้มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละครั้ง
2. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ
3. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยให้กับบุคลากร
4. ประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย
5. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้
6. ให้ผู้ใช้งานมีส่วนร่วมในการ ติดตามประเมินผล และสำรวจความต้องการที่เปลี่ยนไปเสมอๆ
7. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัย
8. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของสภากาชาดไทยและข้อตกลงระหว่างประเทศอย่างเคร่งครัด

ส่วนที่ 5 นโยบายการดำเนินการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

1. ระบบป้องกันผู้บุกรุก (IPS/IDS System) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุกสิ่งที่ทำการตรวจสอบ

2. ระบบไฟร์วอลล์(Firewall System) มีการดำเนินการตรวจสอบระบบป้องกันการบุกรุกอย่างน้อยเดือนละ 1 ครั้ง และมีการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์สิ่งที่ต้องตรวจสอบ

3. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต หรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์ มีการดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต

ส่วนที่ 6 นโยบายคุ้มครองข้อมูลส่วนบุคคล

ตามที่คณะกรรมการธุรกรรมทางอิเล็กรอนิกส์ ได้มีประกาศ เรื่อง “แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553” โดยอาศัยอำนาจตามความในมาตรา 6, 7 และ 8 ใน “พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549” มีสาระสำคัญดังนี้

1. ให้หน่วยงานจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร ประกอบด้วย การเก็บข้อมูลเฉพาะส่วนที่จำเป็น ระบุวัตถุประสงค์การนำไปใช้ชัดเจน แสดงถึงมาตรฐานในการรักษาข้อมูล เป็นต้น
2. ให้หน่วยงานจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการเช่นข้อมูลเบื้องต้น เจ้าของหน่วยงาน การนำข้อมูลไปใช้ การจัดเก็บรวบรวม การเชื่อมโยงกับหน่วยงานอื่นๆ การเปิดเผยข้อมูลส่วนบุคคล การเปิดเผยข้อมูลการใช้บริการ การจัดเก็บและ การเข้าถึง เป็นต้น
3. หากหน่วยงานได้รับการรับรองว่าปฏิบัติตาม 1,2 ได้มาตรฐาน และได้รับการรับรอง ให้แสดงเครื่องหมายการรับรองด้วย
4. ให้หน่วยงานกำหนดเรียกชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจน มีการระบุวัน เดือน ปี และการแก้ไข ปรับปรุงล่าสุด เป็นต้น

ข้อมูลอ้างอิง

https://ictlawcenter.etda.or.th/files/law/file/33/5a42315f04a4f439866e879220ff7227.pdf

กฎหมายใหม่ที่เกี่ยวข้อง
พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พรบ.คุ้มครองข้อมูลส่วนบุคคล

สนช. มีมติเห็นชอบกฎหมายดิจิทัล 2 ฉบับ ‘พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์’ และ ‘พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล’ เมื่อวันที่ 28 กุมภาพันธ์ 2562 การเตรียมนำทูลเกล้าฯ ถวายเพื่อลงพระปรมาภิไธย ก่อนประกาศลงราชกิจจานุเบกษาเพื่อประกาศใช้เป็นกฎหมายต่อไป

หลักการสำคัญ ที่ต้องมี พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ เพราะปัจจุบันการให้บริการสำคัญต่าง ๆ ใช้ระบบดิจิทัล ซึ่งมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ การโจมตีระบบจากอาชญากรคอมพิวเตอร์ ซึ่งอาจกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที กฎหมายนี้จึงมีการกำหนด หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure : CII) ทั้งหน่วยงานของรัฐและเอกชน ตลอดจนกำหนดให้มีมาตรฐานและ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถบริการได้อย่างต่อเนื่อง

กฎหมายใหม่ที่เกี่ยวข้อง

โครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ได้กำหนดไว้ 7 ด้าน ได้แก่

1. ด้านความมั่นคง
2. บริการภาครัฐที่สำคัญ
3. การเงิน-การธนาคาร
4. เทคโนโลยีสารสนเทศและโทรคมนาคม
5. ระบบขนส่งและโลจิสติกส์
6. พลังงาน-สาธารณูปโภค
7. สาธารณสุข

ประโยชน์ที่ประชาชนจะได้จาก พ.ร.บ.ไซเบอร์ มี 3 ข้อ ได้แก่

1. ลดความเสี่ยงและผลกระทบจากการที่หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ ที่ไม่สามารถให้บริการประชาชนได้
2. มีหน่วยงานหลักรับหน้าที่เป็นเจ้าภาพในการช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ ในการรับมือภัยคุกคามไซเบอร์
3. มีการสนับสนุนในการให้ความรู้และฝึกอบรมบุคลากร เพื่อให้รองรับการปฏิบัติหน้าที่

กฎหมายใหม่ที่เกี่ยวข้อง

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ทำไมต้องคุ้มครองข้อมูลส่วนบุคคล

ความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวมข้อมูล การใช้ การเปิดเผยข้อมูลส่วนบุคคล ซึ่งกระทำได้โดยง่ายและรวดเร็ว ทำให้มีการละเมิดสิทธิข้อมูลส่วนบุคคล และก่อให้เกิดความเสียหายต่อตัวบุคคล

สาระสำคัญ

1. บุคคลเจ้าของข้อมูล ต้องให้ความยินยอม การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล
2. ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือมีใครเข้าถึงได้โดยมิชอบ
3. บุคคลเจ้าของข้อมูล มีสิทธิถอนความยินยอม หรือขอให้ลบหรือทำลายข้อมูลได้ เมื่อถูกนำไปใช้ในทางไม่ชอบด้วยกฎหมาย

หน่วยงานที่เกี่ยวข้อง

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- กำหนดมาตรฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ให้ความรู้และการฝึกอบรมแก่หน่วยงานรัฐ เอกชน และบุคคลทั่วไป ในการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการผู้เชี่ยวชาญ

- พิจารณาเรื่องร้องเรียนเมื่อมีการละเมิด
- ตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล
- ไกล่เกลี่ยข้อพิพาท

คนไทยได้อะไรจาก พ.ร.บ.คุ้มครองข้อมูลฯ

1. ป้องกันการล่วงละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคล
2. ปกป้องความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล และความเดือดร้อนรำคาญ
3. สร้างกลไก หรือมาตรฐานการกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล
4. สามารถฟ้องเรียกค่าสินไหมทดแทนกรณีถูกละเมิดข้อมูลส่วนบุคคล

สรุป

"พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์"

ทำไมต้องมี พ.ร.บ. ไซเบอร์

เพื่อปกป้องระบบคอมพิวเตอร์และโครงข่าย IT ของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ หรือ บริการที่สำคัญของประเทศมีความมั่นคงปลอดภัยสามารถให้บริการได้เป็นปกติ และหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ ได้อย่างทันท่วงที

สาระสำคัญกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

1. กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐ มีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์
2. มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ
3. มีการร่วมมือและประสานงานกันและกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้ จนทำให้ประชาชนเดือดร้อน

หน่วยงานหลัก ๆ

หน่วยงานควบคุมหรือกำกับดูแล

ดูแลการดำเนินงานของหน่วยงานรัฐหรือโครงสร้างพื้นฐานสำคัญให้มีมาตรฐาน เช่น ธนาคารแห่งประเทศไทย กำกับดูแลสถาบันการเงิน กสทช.กำกับดูแลผู้ให้บริการโทรคมนาคม

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เป็นศูนย์กลางเฝ้าระวังความปลอดภัยไซเบอร์ของประเทศ และให้การช่วยเหลือในการป้องกันและรับมือเมื่อเกิดภัยคุกคามในระดับร้ายแรง

ภัยคุกคามทางไซเบอร์ระดับร้ายแรง

ระบบในการให้บริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานถูกโจมตี จนไม่สามารถให้บริการได้

ภัยคุกคามทางไซเบอร์ระดับวิกฤติ

ระบบบริการพื้นฐานที่สำคัญถูกโจมตี ไม่สามารถให้บริการได้เป็นวงกว้าง กระทบกับชีวิตและความปลอดภัยของประชาชนจำนวนมาก และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ

ประชาชนได้อะไรจาก พ.ร.บ. ไซเบอร์

1. ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญมีความปลอดภัย สามารถให้บริการได้ต่อเนื่อง
2. มีแนวทางในการรับมือภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบเป็นวงกว้างและกลับมาทำงานได้อย่างรวดเร็ว
3. มีการจัดตั้งหน่วยงานขึ้นมาดูแลมาตรฐานด้านความปลอดภัยไซเบอร์ และให้ความช่วยเหลือแก่หน่วยงานโครงสร้างพื้นฐานที่สำคัญ
4. เมื่อเกิดภัยคุกคามร้ายแรง การเข้าไปแก้ไขปัญหาที่ต้องเข้าถึงทรัพย์สิน จะต้องใช้คำสั่งศาลเพื่อคุ้มครองสิทธิ์

จบบริบูรณ์

ตัวอย่าง KPI ของ Job ที่เป็น Developer และ Product Support

Sample of Key Performance Indicator/Business contribution	Name :
Job catetory ◆**Software Technology (Development, Product Support)**	Level

Level ITSS	Business contribution																	
	Responsibility			Ability				Project Exp. (value)					System Complexity						Team size
	Task	Team	Project (Task,Team,Time,Cost)	work under close support (need guide)	work independently	supervise team	could manage project, teams and resources	S (< 1M)	SM (1 - 2.5M)	M (2.5 - 5M)	ML (5 - 10M)	L (> 10M)	online or batch	Mission Critical (24x7, etc.)	Number of Interface	Number of User	Multi Platform, Database	Multi site	A number of development team members during peak periods
4 (JC11-JC12)	**X**	**X**	**X**		**X**	**X**	**X**		**5**	**3**	**2**	**1**	O	**X**	>50	>100	**X**	**X**	5
3 (JC9-JC10)	**X**	**X**			**X**	**X**		**5**	**3**	**2**			O	**X**	>10	<100	**X**	**X**	< 5
2 (JC8-JC9)	**X**				**X**								O		>5	<10	**X**		-
1 (JC6-JC7)				**X**									B		<5				-

ตัวอย่าง Skill Analysis

25 October 2015

Ability to perform

ITX		Consult	Develop					BA/SA		DBA	SE	English	Test				
Resources		Dev&Imp.	Biz	Handler	ETL	DB	Data	IC	WkFlow		Deploy	Skill	Auto-Test	Manual-Test			
	Name	Mgmt	Rules				Channel	Config	Config					B	H	E	I
1	NS	4	4	2	4	2	1	4	2		4	4					
2	WB	3	4	4	2	2	4	4	3		4	2					x
3	ET	3	4	3	2	4	4	2		3	3	2.5					3
4	RJ					2	1					4	4				2
5	PR		3.5	1		2		3				4					3
6	BO		3	2	1	2	3	2			2	2					3
7	LM		3	1	2	1						4					3
8	OY		1	1	3	2						2					3
9	TP										3	3					
10	JO										3	3					
11	NI				2		2	1			2	2					
12	PL		3		3	3		2			3	3					3
13	PI		1					1									2
14	PA																2

Ability Level to perform Job

1	Has Knowledge, never perform
2	Can perform w/ support
3	Can perform independently
4	Can perform and teach others

English Ability

1	พอรู้แต่สื่อสารไม่ได้
2	สื่อสารได้แต่ต้องมีคนช่วยบ้าง
3	สามารถสื่อสารได้เอง
4	สื่อสารได้ในระดับดี