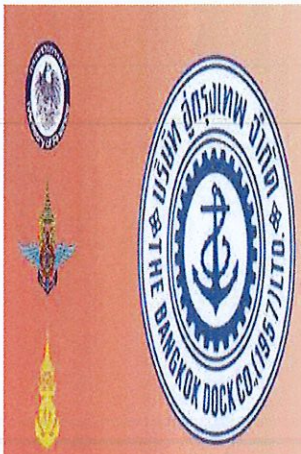
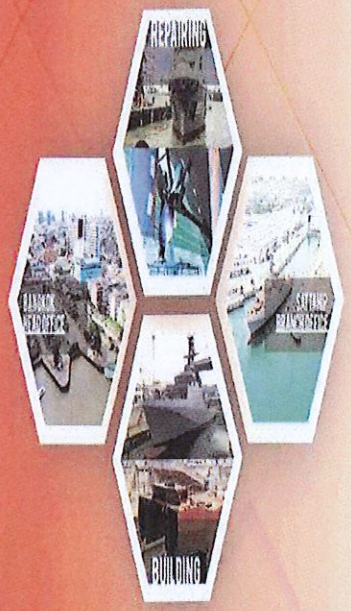


THE BANGKOK DOCK COMPANY



รัฐวิสาหกิจในความควบคุมของกองทัพเรือ
สังกัดกระทรวงกลาโหม

คู่มือปฏิบัติงาน

แผนกเทคโนโลยีดิจิทัล

ปรับปรุง 2565

BANGKOK DOCK NEXT

สารบัญ

คำนำ

บริษัท อู่กรุงเทพ จำกัด เป็นรัฐวิสาหกิจตามนโยบายพิเศษของรัฐ จัดอยู่ในประเภทยุทธปัจจัย สาขาอุตสาหกรรม อยู่ในความควบคุมของกองทับเรือสังกัดกระทรวงกลาโหม และได้ให้ความสำคัญต่อการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้กับการดำเนินงานภายในองค์กรตามกรอบนโยบายสารสนเทศของประเทศและตามมติคณะรัฐมนตรี

แผนกสารสนเทศของบริษัท มีหน้าที่ในการพัฒนาระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการตามนโยบายของรัฐและเพื่อให้เกิดผลสัมฤทธิ์ในการบริหารจัดการภายในบริษัท

ดังนั้น แผนกฯจึงได้ถ่ายทอดกระบวนการ ขั้นตอน วิธีดำเนินการ ขอบเขตและแนวทางปฏิบัติจัดทำคู่มือปฏิบัติของแผนก เพื่อใช้เป็นแนวทางสำหรับผู้ปฏิบัติงานในแผนกบุคลากรที่เกี่ยวข้อง ได้รับความสะดวก รวดเร็วในการค้นคว้า และสามารถปฏิบัติงานได้ถูกต้อง

แผนกสารสนเทศหวังเป็นอย่างยิ่งว่า คู่มือปฏิบัติงานเล่มนี้จะเป็นประโยชน์และเกิดผลสัมฤทธิ์ของงานแก่ผู้ปฏิบัติงานและผู้ที่เกี่ยวข้องต่อไป

แผนกเทคโนโลยีสารสนเทศ

กันยายน 2566

บทที่ 1 บทนำ

1.1 วิสัยทัศน์ด้านเทคโนโลยีดิจิทัล

“มุ่งเน้นการนำเทคโนโลยีดิจิทัลมาพัฒนาบริษัทสู่ความเป็นอู่เรือที่มีศักยภาพในการบริหารจัดการระดับสากล และเป็น Smart Dockyard”

1.2 พันธกิจวิสัยทัศน์ด้านเทคโนโลยีดิจิทัล

“สนับสนุนและเพิ่มศักยภาพในการบริหารจัดการด้านสารสนเทศ ปรับปรุงระบบเทคโนโลยีสารสนเทศเพื่อรองรับการเรียนรู้ การสร้างนวัตกรรม และการสื่อสารเพื่อการเป็น Smart Dockyard และ Thailand 4.0”

1.4 วัตถุประสงค์

1. เพื่อจัดทำแผนการดำเนินงานด้านเทคโนโลยีดิจิทัล ให้สอดคล้องกับแผนวิสาหกิจ และนโยบายภาครัฐ
2. เพื่อนำเทคโนโลยีดิจิทัลที่เหมาะสมมาสนับสนุนการทำงานขององค์กร
3. เพื่อพัฒนาระบบเทคโนโลยีดิจิทัล เข้าสู่ระบบ Smart Dockyard และ Thailand 4.0
4. เพื่อเชื่อมโยงระบบเครือข่ายทั้งภายในและภายนอกองค์กรอย่างมีประสิทธิภาพ
5. เพื่อสร้างนวัตกรรมและการจัดการความรู้ในองค์กร

1.4 โครงสร้างแผนกเทคโนโลยีสารสนเทศ

1.5 ขอบข่ายหน้าที่ตามมาตรฐานกำหนดตำแหน่ง

ตำแหน่งงาน : หัวหน้าแผนกเทคโนโลยีสารสนเทศ

ลักษณะงานโดยทั่วไป

สายงานนี้มีลักษณะงานปฏิบัติเกี่ยวกับการพัฒนาแผนปฏิบัติการดิจิทัลและจัดทำแผนปฏิบัติการเทคโนโลยีสารสนเทศ ให้สามารถตอบสนองการปฏิบัติภาระกิจของหน่วยงานตลอดจนปรับเปลี่ยนเพื่อให้มีความสัมฤทธิ์ผลอย่างเหมาะสม

หน้าที่ความรับผิดชอบหลัก

- ปฏิบัติงานในฐานะหัวหน้างาน ซึ่งต้องกำกับ แนะนำ ตรวจสอบการปฏิบัติงานของผู้ร่วม
- ปฏิบัติงาน โดยใช้ความรู้ความสามารถ ประสบการณ์ และความชำนาญงานสูงมากในงานวิชาการคอมพิวเตอร์ ปฏิบัติงานที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากมาก และ
- ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย หรือ ปฏิบัติงานในฐานะผู้ปฏิบัติงานที่มีประสบการณ์ โดยใช้ความรู้ความสามารถประสบการณ์ และความชำนาญในงานสูงมากในงานวิชาการคอมพิวเตอร์
- ปฏิบัติงานที่ต้องตัดสินใจหรือแก้ปัญหาที่ยากมาก และปฏิบัติงานอื่นตามที่ได้รับมอบหมายโดยมีลักษณะงานที่ปฏิบัติในด้านต่าง ๆ ดังนี้

ด้านการปฏิบัติการ

- ศึกษาวิเคราะห์ ให้คำปรึกษาหรือข้อเสนอแนะในการพัฒนาระบบคอมพิวเตอร์ระบบสารสนเทศที่เกี่ยวข้อง เพื่อร่วมพัฒนางานคอมพิวเตอร์และเทคโนโลยีสารสนเทศให้ทันสมัยและก้าวทันเทคโนโลยีอยู่เสมอ
- ช่วยกำกับติดตามการดำเนินงาน หรือพิจารณาเสนอแนะให้ความเห็นเกี่ยวกับการพัฒนาระบบระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบงานประยุกต์ และระบบงานสารสนเทศ เพื่อให้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศในหน่วยงานทันสมัยและตอบสนองการปฏิบัติงานในหน่วยงานได้อย่างเต็มประสิทธิภาพ
- จัดทำประเด็นข้อเสนอ สรุปรายงานในการนำเสนอต่อที่ประชุมคณะกรรมการชุดต่าง ๆ เพื่อกำหนดแนวทาง หลักเกณฑ์และวิธีการดำเนินงานด้าน ระบบระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ระบบงานประยุกต์และระบบงานสารสนเทศ

- จัดทำและพัฒนาระบบงานประยุกต์ระบบสารสนเทศ ระบบการเชื่อมโยงแลกเปลี่ยนข้อมูลระบบฐานข้อมูลและระบบคลังข้อมูลที่มีขอบข่ายกว้าง
  เพื่อสนับสนุนการปฏิบัติงานด้านสารสนเทศที่มีความซับซ้อนในหน่วยงาน
- กำกับ บริหาร การพัฒนาระบบงานต่างๆ ให้เป็นไปตามข้อกำหนด/สัญญา
- พิจารณาวิธีการหลักเกณฑ์การกำหนดคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย ระบบงานประยุกต์และระบบสารสนเทศการจัดการระบบการทำงานเครื่องการติดตั้งระบบเครื่อง
  เพื่อให้ได้อุปกรณ์คอมพิวเตอร์ที่เป็นมาตรฐานเดียวกันทั้งหน่วยงานและตรงตามความต้องการ
  ลักษณะการใช้งานของหน่วยงาน

ด้านการวางแผน

- วางแผนหรือร่วมดำเนินการวางแผนงาน โครงการของหนวยงานระดับสำนักหรือกอง
- มอบหมายงาน แก้ไขปญหาในการปฏิบัติงานและติดตามประเมินผลเพื่อให้เป็นไปตามเป้าหมายที่กำหนด

ด้านการประสานงาน

- ประสานสัมพันธ์กับสมาชิกในทีมงานโดยมีบทบาทในการชี้แนะ จูงใจ
  ทีมงานหรือหน่วยงานอื่นในระดับกองหรือสำนักเพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้
- ชี้แจงให้ข้อคิดเห็นในที่ประชุมคณะกรรมการหรือคณะทำงานต่างเพื่อเป็นประโยชน์และเกิดความร่วมมือในการ ดำเนินงานร่วมกัน
- ด้านการบริการให้คำปรึกษาแนะนำแก่หน่วยงานราชการ เอกชน เกี่ยวกับการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบงานประยุกต์
  และระบบงานสารสนเทศเพื่อให้การพัฒนางานด้านคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ
- อำนวยการฝึกอบรม หรือถ่ายทอดความรู้ให้แก่เจ้าหน้าที่ระดับรองลงมา
  เพื่อเป็นที่ปรึกษาและร่วมพัฒนาบุคลากรที่มีคุณภาพให้แก่หน่วยงาน และปฏิบัติหน้าที่อื่น ๆ
  ที่เกี่ยวข้องตามที่ได้รับมอบหมาย
- พิจารณากำหนดหลักสูตรการฝึกอบรมหรือถ่ายทอดความรู้ สนับสนุนการใช้ระบบงานที่
- พัฒนาแก่เจ้าหน้าที่ผู้ใช้งาน หรือเจ้าหน้าที่ระดับรองลงมา

ตำแหน่งงาน : พนักงานเทคโนโลยีสารสนเทศ

ลักษณะงานโดยทั่วไป

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับต้น ที่ต้องใช้ความรู้ความสามารถทางวิชาการ ในการทำงานปฏิบัติงานเกี่ยวกับ วิทยาการคอมพิวเตอร์ ภายใต้การกำกับ แนะนำ ตรวจสอบ และปฏิบัติงานอื่นตามที่ได้รับมอบหมายโดยมีลักษณะงานที่ปฏิบัติในด้านต่าง ๆ ดังนี้

ด้านการปฏิบัติการ

- ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล โปรแกรมระบบปฏิบัติการ โปรแกรมสำเร็จรูป ระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง เพื่ออำนวยการให้งานเทคโนโลยีสารสนเทศในความรับผิดชอบดำเนินไปได้อย่างราบรื่นและสอดคล้องกับความต้องการของหน่วยงาน
- ทดสอบคุณสมบัติด้านเทคนิคของระบบ เพื่อให้ระบบมีคุณสมบัติที่ถูกต้องตรงตามความต้องการและสภาพการใช้งานของหน่วยงานอยู่เสมอ
- เพื่อสนับสนุนการปฏิบัติงานเทคโนโลยีสารสนเทศให้ดำเนินไปได้อย่างราบรื่น
- ช่วยรวบรวมข้อมูลและวิเคราะห์ความต้องการของระบบงานประยุกต์และระบบข้อมูลของหน่วยงานที่ไม่ซับซ้อน เพื่อพัฒนาระบบงานเทคโนโลยีสารสนเทศในหน่วยงานให้มีประสิทธิภาพและตรงตามความต้องการของหน่วยงานมากที่สุด
- ช่วยรวบรวมข้อมูลและวิเคราะห์ ออกแบบ และพัฒนาระบบงานประยุกต์ เพื่อให้ได้ระบบงานประยุกต์ที่ตรงตามคุณลักษณะและความต้องการของหน่วยงาน
- รวบรวมข้อมูลประกอบการกำหนดคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย ระบบงานประยุกต์และระบบสารสนเทศ การจัดการระบบการทำงานเครื่อง
- การติดตั้งระบบเครื่อง เพื่อให้ได้อุปกรณ์คอมพิวเตอร์ที่เป็นมาตรฐานเดียวกันทั้งหน่วยงานและตรงตามความต้องการ ลักษณะการใช้งานของหน่วยงาน

ด้านการวางแผน

- วางแผนการทำงานที่รับผิดชอบร่วมดำเนินการวางแผนการทำงานของหน่วยงานหรือ
- โครงการเพื่อให้การดำเนินงานเป็นไปตามเป้าหมายผลสัมฤทธิ์ที่กำหนด

ด้านการประสานงาน

- ประสานงานทำงานร่วมกันทั้งภายในและภายนอกทีมงานหรือหน่วยงาน เพื่อให้เกิดความ
- ร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้
- ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงาน ที่เกี่ยวข้อง เพื่อ
- สร้างความเข้าใจหรือความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย
- ด้านการบริการ

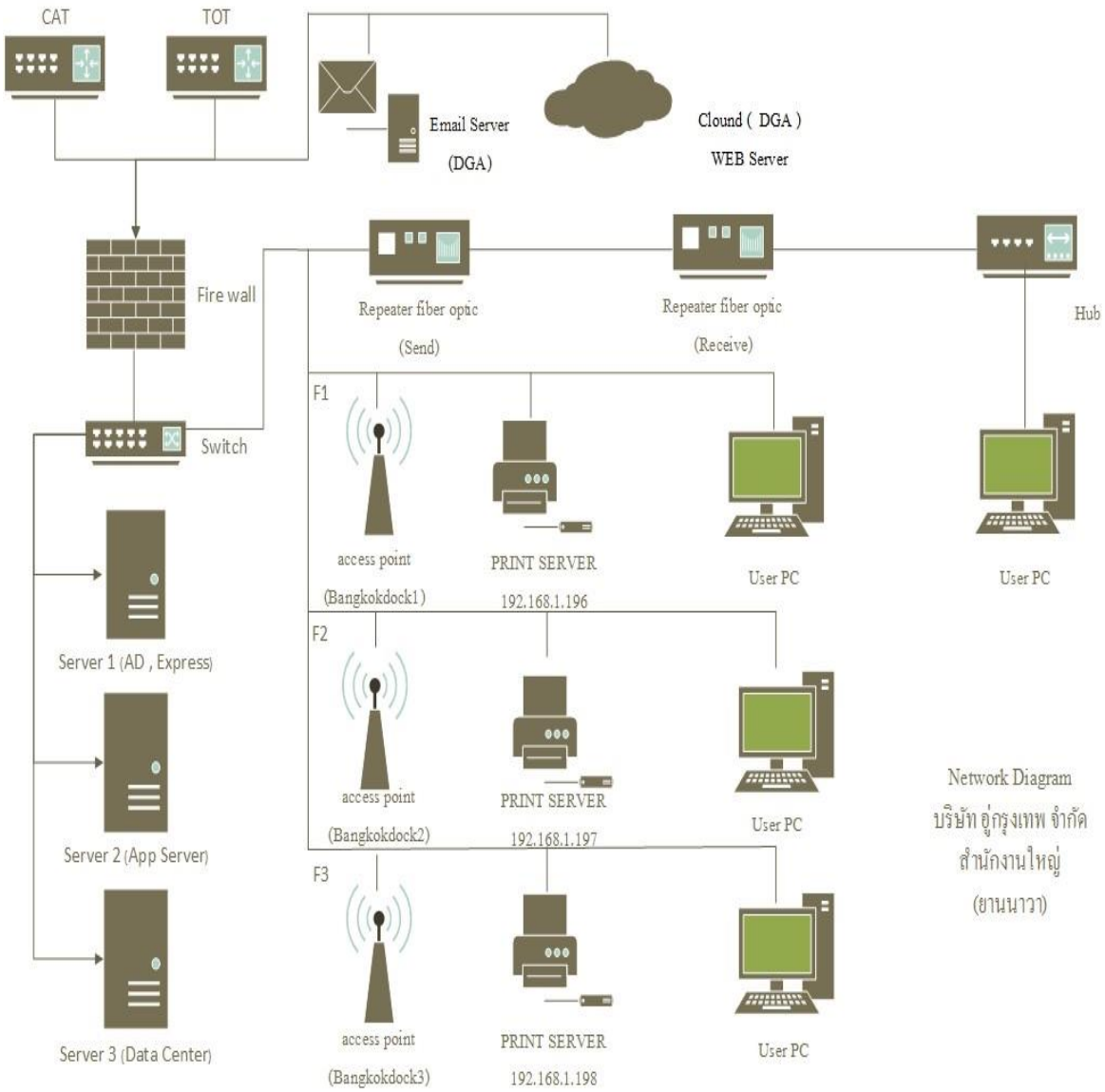
- ช่วยจัดทำคู่มือระบบและคู่มือผู้ใช้ เพื่ออำนวยความสะดวกแก่ผู้ใช้ให้สามารถใช้งาน
- คอมพิวเตอร์ได้ด้วยตนเอง
- ดำเนินการฝึกอบรมหรือถ่ายทอดความรู้ สนับสนุนการใช้ระบบงานที่พัฒนา แก่เจ้าหน้าที่
- ผู้ใช้งาน หรือเจ้าหน้าที่ระดับรองลงมา
- ร่วมกับผู้ใช้ในการนำระบบไปใช้ในการปฏิบัติงาน เพื่อช่วยเหลือผู้ใช้หากมีปัญหา
- หรือข้อสงสัยในการใช้งานเครื่องคอมพิวเตอร์ และปฏิบัติงานอื่นที่เกี่ยวข้องตามที่ได้รับมอบ

บทที่ 2
การบริหารจัดการเทคโนโลยีสารสนเทศในองค์กร

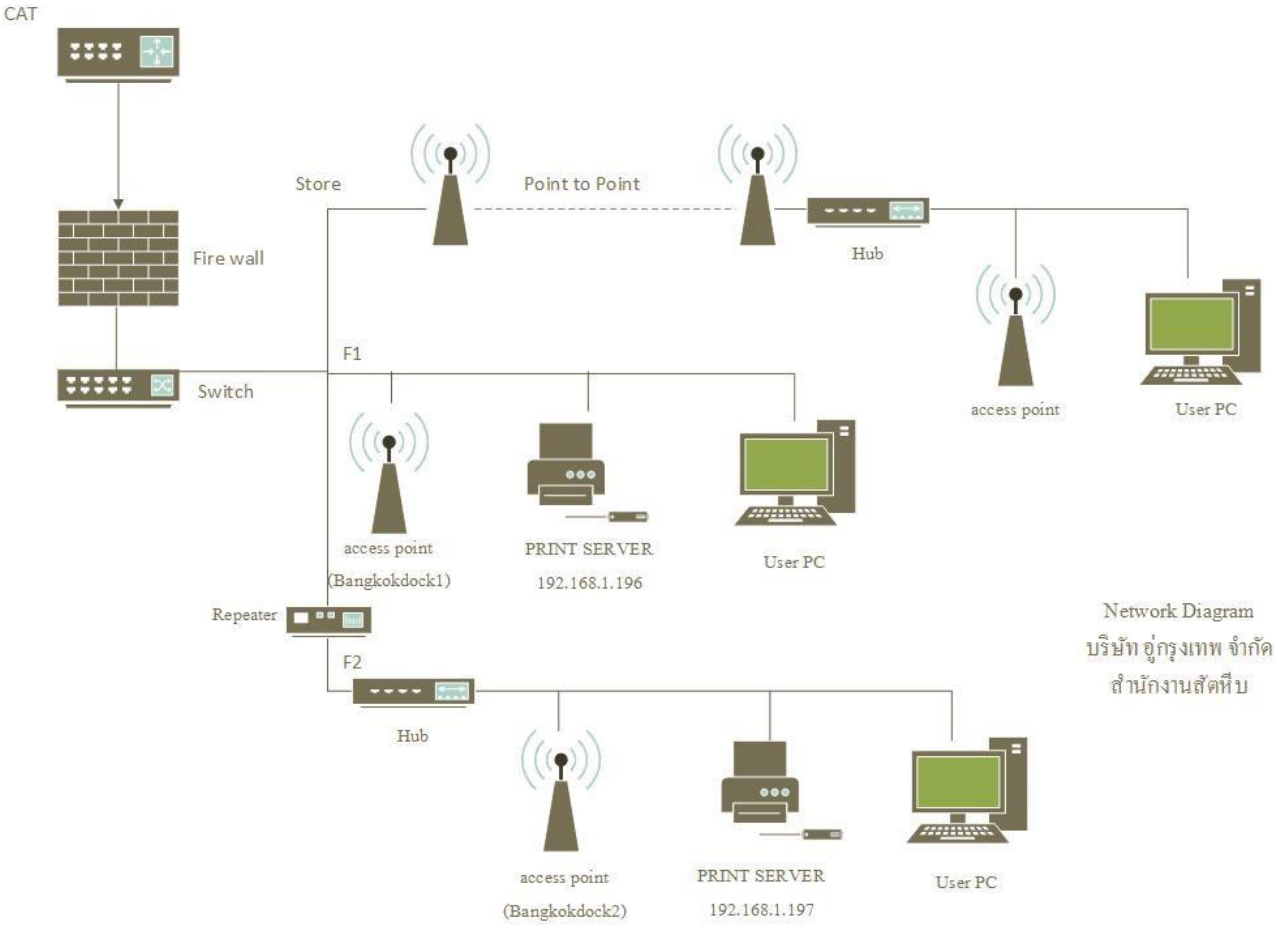
2.1 ระบบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ ในปัจจุบัน

โครงสร้างพื้นฐานทางด้านคอมพิวเตอร์และอุปกรณ์ต่อพ่วงของ บอท. ประกอบด้วย

2.1.1 สำนักงานใหญ่ กรุงเทพ



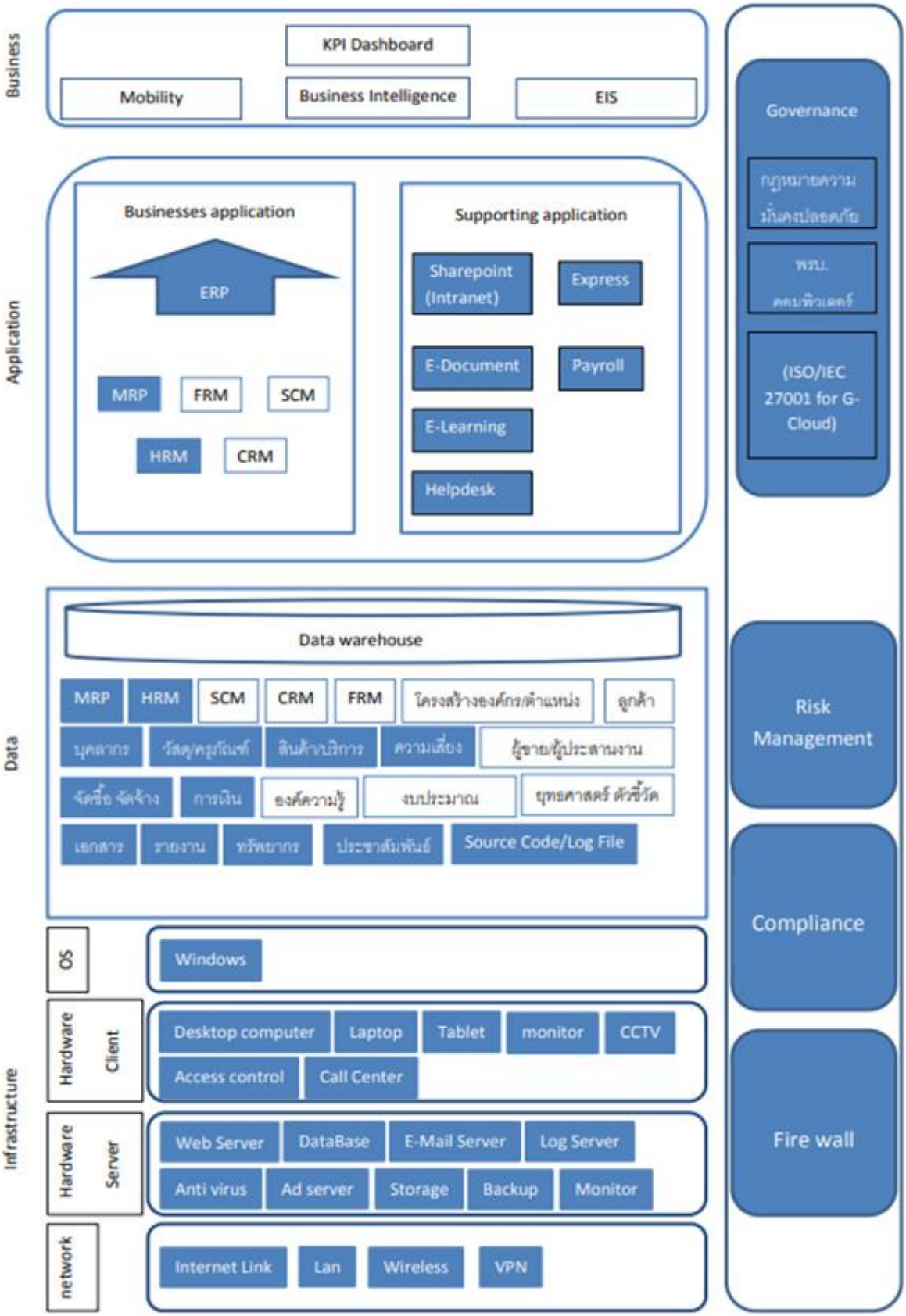
2.1.2 สำนักงาน สัตหีบ



2.1.3 ระบบการเชื่อมเทคโนโลยีสารสนเทศ ระหว่างสำนักงานส่วนกลางและสาขา ผ่านระบบ VPN

ด้านฮาร์ดแวร์บอท.ส่งเสริมสนับสนุนให้หน่วยงานภายในใช้อุปกรณ์เครือข่ายที่มีมาตรฐานเดียวกัน ตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ประจำปี พ.ศ. 2560
เพื่อความสะดวกในการจัดการ และการบำรุงรักษา
มีการเชื่อมโยงเครือข่ายสารสนเทศส่วนกลางสนับสนุนการใช้ทรัพยากรในระบบคอมพิวเตอร์ร่วมกันโดยมีการใช้งานผ่านระบบเครือข่ายร่วมกัน เช่น เครื่องพิมพ์เลเซอร์, เครื่องพิมพ์สี , เครื่องเขียนกราฟ (plotter) , เครื่องสแกน เป็นต้น
การจัดให้มีส่งเสริมให้มีการใช้งานเครือข่าย Intranet ภายในหน่วยงานให้มีการใช้งานอย่างมีประสิทธิภาพ
มีการเชื่อมโยงระหว่างสาขาผ่านระบบ VPN เพื่อจัดทำศูนย์ข้อมูล (Data Center) ในการจัดการด้าน MIS หรือ Management Information System อย่างมีประสิทธิภาพ

2.2 ระบบงานสารสนเทศ ของ บอท. ตามแผนทางสถาปัตยกรรมองค์กร (Enterprise Architecture)


Business
KPI Dashboard
Mobility
Business Intelligence
EIS
Application
Businesses application
ERP
MRP
FRM
SCM
HRM
CRM
Supporting application
Sharepoint (Intranet)
Express
E-Document
Payroll
E-Learning
Helpdesk
Data
Data warehouse
MRP
HRM
SCM
CRM
FRM
โครงสร้างองค์กร/ตำแหน่ง
ลูกค้า
บุคลากร
วัสดุ/ครุภัณฑ์
สินค้าบริการ
ความเสี่ยง
ผู้ขาย/ผู้ประสานงาน
จัดซื้อ จัดจ้าง
การเงิน
องค์ความรู้
งบประมาณ
ยุทธศาสตร์ ตัวชี้วัด
เอกสาร
รายงาน
ทรัพยากร
ประชาสัมพันธ์
Source Code/Log File
Infrastructure
OS
Windows
Hardware Client
Desktop computer
Laptop
Tablet
monitor
CCTV
Access control
Call Center
Hardware Server
Web Server
DataBase
E-Mail Server
Log Server
Anti virus
Ad server
Storage
Backup
Monitor
network
Internet Link
Lan
Wireless
VPN
Governance
กฎหมายความมั่นคงปลอดภัย
พรบ. คอมพิวเตอร์
(ISO/IEC 27001 for G-Cloud)
Risk Management
Compliance
Fire wall

- EIS ย่อมาจาก executive information system แปลว่า ระบบสารสนเทศเพื่อผู้บริหารระดับสูง หมายถึง การนำสารสเนศหรือข้อมูลต่าง ๆ มาเก็บไว้ในรูปแบบที่ผู้บริหารสามารถใช้ได้สะดวก
- KPI Dashboard เป็นการติดตามผลการดำเนินงารระดับองค์กรแบ่งเป็น การติดตามผลการดำเนินงานระดับองค์กร ระดับหน่วยงานและระดับบุคคล ผ่านออนไลน์โดยนำความก้าวหน้าของเทคโนโลยีสารสนมาใช้ในการติดตามความก้าวหน้าของผลการดำเนินงานเปรียบเทียบเป้าหมายที่กำหนด
- **Mobility** คือ อุปกรณ์ที่ใช้ในการติดต่อสื่อสาร ผ่านบนเครือข่ายไร้สาย เช่น Laptop, Smart Phone ,Tablet เป็นต้น ที่ในสังคมยุคปัจจุบันนี้มีการใช้ อุปกรณ์พกพาเหล่านี้กันอย่างแพร่หลาย เพราะอุปกรณ์พกพานี้ช่วยในเรื่องความสะดวกสบายสามารถที่จะทำงานได้แบบไร้พรมแดน รวดเร็ว สะดวกในการพกพา
- Business Intelligence (BI) คือการใช้เทคโนโลยีต่างๆ
  เพื่อวิเคราะห์และประมวลผลข้อมูลที่ได้มาเพื่อใช้ในการทำธุรกิจ ทั้งการบริหารจัดการ เสนองาน ไปจนถึงการวางแผนงานในช่วงเวลาจำกัด โดยมีหลักการทำงานดังนี้
  - การเก็บข้อมูลจากแหล่งข้อมูล เช่น เก็บข้อมูลจากการออเดอร์ของลูกค้า ข้อมูลเพศ อายุ และอื่นๆ
  - นำข้อมูลมาประมวลผล ด้วยเครื่องมือด้าน Business Intelligence ว่าใช้งานข้อมูลที่ประมวลผลแล้ว
- ERP (Enterprise resource planning) คือ การวางแผนบริหารธุรกิจขององค์กร
  เพื่อให้องค์กรนั้นสามารถใช้ทรัพยากรที่มีได้อย่างมีประสิทธิภาพสูงสุด โดยปัจจุบัน บอท.มีโครงการพัฒนาระบบ ERP (Enterprise resource planning) คือ การวางแผนบริหารธุรกิจขององค์กร
  เพื่อให้องค์กรนั้นสามารถใช้ทรัพยากรที่มีได้อย่างมีประสิทธิภาพสูงสุด มีองค์ประกอบดังนี้คือ **MRP** หรือ Manufacturing Resource Planning , **FRM** หรือ Finance Resource Management , **SCM** หรือ Supply Chain Management , **CRM** หรือ Customer Relationship Management และ **HRM** หรือ Human Resource Management

บทที่ 3
การกำกับดูแลด้านเทคโนโลยีดิจิทัลและแผนปฏิบัติการดิจิทัลขององค์กร
(Digital Governance and Roadmap)

3.1 กำหนดกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance)

- กระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance)
- รัฐวิสาหกิจกำหนดกรอบการกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม (Benefits Delivery and Resource Optimization Framework Setting)
    - การกำหนดความรับผิดชอบ (Responsibility)
    - กลยุทธ์ขององค์กรที่สอดคล้องกับความสามารถด้านเทคโนโลยีดิจิทัล (Strategy)
    - การจัดหา (Acquisition) ที่มีประสิทธิภาพ
      และการประเมินประสิทธิผล/ความคุ้มค่าของการลงทุนด้านเทคโนโลยีดิจิทัล (Evaluation of Investment and Services portfolios)
- รัฐวิสาหกิจกำหนดกรอบการกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส (Performance Measurement and Stakeholder Transparency Framework Setting)
    - ความสอดคล้องกับระเบียบและข้อบังคับ (Conformance) การปฏิบัติตาม กฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล
    - ประสิทธิภาพการดำเนินงาน (Performance)
      การตรวจติดตามการนำไปปฏิบัติตามกระบวนการ
- รัฐวิสาหกิจการกำหนดกรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Risk Optimization Framework Setting)
- รัฐวิสาหกิจมีการสื่อสารหลักการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance guiding principle Communications)
- มีการถ่ายทอดกระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล
  แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
  โดยมีการแสดงการวิเคราะห์ที่ชัดเจน
  และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome)
  ของกระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล
  และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน

การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

แนวทางกำหนดกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance) โดยการจัดทำกฎบัตรคณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล รองรับการดำเนินงานของคณะกรรมการบริษัท ที่ได้รับการแต่งตั้งเพื่อดำเนินการด้านการพัฒนาเทคโนโลยีดิจิทัลขององค์กร โดยมีการพิจารณาเสนอทบทวนทุกรอบปีเพื่อความทันสมัยของแนวทางการกำกับดูแล

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	**การพิจารณาแผนแม่บทด้านการพัฒนาเทคโนโลยีดิจิทัล**														
	1.6 กฎบัตรคณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล		ดำเนินการทบทวน / ปรับปรุงได้ทันต่อการใช้งานในเวลาที่กำหนด												
	1.6.1 คณะทำงานการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล												⟷	⟷	
	1.6.2 คณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล													⟷	
	1.6.3 คณะกรรมการบริษัท อู่กรุงเทพ จำกัด														⟷

3.2 แผนปฏิบัติการดิจิทัล (Digital Roadmap) และแผนปฏิบัติการประจำปี (Digital Roadmap and Action Plan)

รัฐวิสาหกิจมีการจัดทำแผนปฏิบัติการดิจิทัลระยะ 3- 5 ปี ที่มีความเชื่อมโยงและสอดคล้องกับแผนวิสาหกิจขององค์กร และนโยบายต่าง ๆ เต็มตามศักยภาพของระบบเทคโนโลยีดิจิทัล โดยมุ่งเน้นการนำเทคโนโลยีดิจิทัล มาปรับใช้กับทุกส่วนขององค์กร และทุกส่วนของธุรกิจ (Digital Transformation) ทั้งในส่วนของกระบวนการทำงาน การสร้างสรรค์ผลิตภัณฑ์ การตลาด วัฒนธรรมองค์กร และการกำหนดเป้าหมายการเติบโตในอนาคต เพื่อให้เกิดประสิทธภาพในการดำเนินธุรกิจและสามารถรองรับการเปลี่ยนแปลงได้อย่างรวดเร็ว รวมถึงในการสร้างธุรกิจใหม่ๆ รูปแบบบริการใหม่ๆ ให้เกิดขึ้น ตลอดจนการบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธภาพ

และมีการบริหารจัดการด้านคุณภาพของการนำเทคโนโลยีดิจิทัลมาใช้
มีการกำหนดรายละเอียดที่ชัดเจนในส่วนของเป้าหมายการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ที่แสดงให้เห็นถึงการปรับเปลี่ยนทั้งในส่วนกระบวนการ (Process) บุคลากร (People) เทคโนโลยี (Technology) มีการดำเนินการเพื่อตอบสนองต่อนโยบายที่สำคัญ โดยมีหลักเกณฑ์ การพิจารณาดังนี้

- Digital Transformation
- Government Integration
- Data Governance and Big Data Management
- Information Security Management
- Business Continuity and Availability Management
- Resource Optimization Management
- ประชาชน/ผู้ใช้บริการได้รับความสะดวกและได้รับการตอบสนองตามความต้องการ

รัฐวิสาหกิจมีการจัดทำแผนปฏิบัติการในระดับองค์กรที่ถ่ายทอดมาจากแผนปฏิบัติการดิจิทัลระยะ 3- 5 ปี มีองค์ประกอบหรือรายละเอียดดังนี้

- มี KPI ที่แสดงถึงความสำเร็จและสะท้อนผลลัพธ์ที่คาดหวัง เช่น
  ระยะเวลาการให้บริการที่ลดลงในระหว่างการดำเนินงาน ณ สิ้นปีบัญชีแรก
  และระยะเวลาที่ลดลงในปีถัดไปหรือเมื่อการดำเนินงานเสร็จสิ้น เป็นต้น
  โดยเป้าหมายมีความท้าทาย ลำดับความสำคัญของแผนงาน / โครงการดังกล่าวอย่างเหมาะสม เช่น กลุ่ม / ลำดับความสำคัญเร่งด่วน กลุ่ม / ลำดับความสำคัญปานกลาง เป็นต้น
- รัฐวิสาหกิจมีกระบวนการจัดทำแผนปฏิบัติการดิจิทัล และแผนปฏิบัติการประจำปี
  และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
  มีการกำหนดรายละเอียดที่ชัดเจนในส่วนของเป้าหมายการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ที่แสดงให้เห็นถึงการปรับเปลี่ยนทั้งในส่วนของ Process People Technology ความเชื่อมโยงและสอดคล้องกับแผนวิสาหกิจขององค์กร และนโยบายต่าง ๆ เต็มตามศักยภาพของระบบเทคโนโลยีดิจิทัล ประกอบด้วย
  - การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร และทุกส่วนของธุรกิจ (Digital Transformation)
  - การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)
  - การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)
  - การบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

(Information Security Management)

- การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)
- การบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management)
- ประชาชน/ผู้ใช้บริการได้รับความสะดวกและได้รับการตอบสนองตามความต้องการ
- การดำเนินการให้มีการปฏิบัติการ หรือ การประกอบธุรกิจที่มีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับและมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรม
- มีการถ่ายทอดกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปี แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดทำแผนปฏิบัติการดิจิทัลและแผนปฏิบัติการประจำปี และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

แนวทางการจัดทำแผนปฏิบัติการดิจิทัล (Digital Roadmap) และแผนปฏิบัติการประจำปี (Digital Roadmap and Action Plan) งโดยคณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลกำกับดูแลให้มีการทบทวนและพัฒนาแนวทางการจัดทำแผนปฏิบัติการดิจิทัล (Digital Roadmap) เพื่อเป็นแนวทางในการนำไปทำแผนปฏิบัติการประจำปีทุกปีเพื่อให้สอดคล้องกับข้อเสนอแนะของนโยบายภาครัฐ และเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1	**การพิจารณาแผนแม่บทด้านการพัฒนาเทคโนโลยีดิจิทัล**														
	1.1 ทบทวนแผนปฏิบัติการดิจิทัล 3-5 ปี	เสนอร่างแผนงาน/คู่มือ	สามารถดำเนินการ												
	1.1.1 คณะทำงานการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล	ต่อผู้บริหาร บอท.และ	ทบทวน / ปรับปรุง												
	1.1.2 คณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล	อนุกรรมการฯ เพื่อให้	ได้ทันต่อการใช้งาน												
	1.1.3 คณะกรรมการบริษัท อู่กรุงเทพ จำกัด	คณะกรรมการบริษัท	และมีความทันสมัย												

บทที่ 4
การสร้างระบบบริหารคุณภาพ (Quality Management System) และการบริหารจัดการโครงการ (Project Management)

รัฐวิสาหกิจที่ครอบคลุมถึงการกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศอย่างเหมาะสม (Benefits Delivery and Resource Optimization Framework Setting) การกำกับดูแลด้านการดำเนินงานให้มีประสิทธภาพและ มีความโปร่งใส (Performance Measurement and Stakeholder Transparency Framework Setting) และการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Optimization Framework Setting) มีการกำหนดขอบเขตและแนวทางในการสร้างระบบบริหารคุณภาพ (Quality Management System) มีการกำหนดขอบเขตและแนวทางในการตรวจสอบด้านเทคโนโลยีดิจิทัล (Digital Audit) หรือ Computer Audit การสื่อสารแนวทางสำหรับระบบการจัดการด้านคุณภาพ (Quality Management System (QMS) Communications) มีกระบวนการจัดการด้านคุณภาพ และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย

- กำหนดขอบเขตการจัดการด้านคุณภาพ
- กำหนดมาตรฐานการจัดการด้านคุณภาพ โดยมีแนวทางการเลือกเครื่องมือ/เทคนิคการจัดการด้านคุณภาพที่ชัดเจน
- การจัดทำ Quality Management Plan พร้อมทั้งการกำหนด บทบาท หน้าที่ ความรับผิดชอบ และอำนาจการตัดสินใจที่เป็นรูปธรรม
- การจัดทำ QMS Good Practices
- การตรวจสอบด้านดิจิทัล (Digital Audit) หรือ Computer Audit

รัฐวิสาหกิจมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการจัดการด้านคุณภาพ และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการจัดทำ QMS Good Practices มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

หลักการของมาตรฐานสากล ISO/IEC 29110 ในปัจจุบัน มีอยู่ด้วยกัน 4 ระดับ คือ Entry Profile, Basic Profile, Intermediate Profile และ Advanced Profile โดยมาตรฐานสากล ISO/IEC 29110 ที่นำมาใช้ในการปรับปรุงกระบวนการทำงานอยู่ในระดับของ Basic Profile (Basic VSEs Profile) ซึ่งเหมาะกับการนำไปใช้ในการบริหารจัดการ และดำเนินโครงการ สำหรับบริษัทหรือองค์กรที่มีขนาดเล็ก (VSEs, Very Small Entities) มาตรฐานสากล ISO/IEC 29110 ระดับ Basic VSE Profile จะมุ่งเน้นไปที่ 2 กระบวนการหลักๆ คือ

1. Project Management (PM) Process
2. Software Implementation (SI) Process

4.1 Project Management (PM) Process เป็นกระบวนการ ที่ใช้ในการวางแผนการดำเนินโครงการ การจัดการทรัพยากรที่จำเป็นต้องใช้ในโครงการ การควบคุมภาพรวมของโครงการ การติดตามความคืบหน้าของโครงการเมื่อเปรียบเทียบกับแผนที่ได้วางไว้ รวมถึงการปรับเปลี่ยนแผนการต่างๆ เพื่อให้เหมาะสมการบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Project Management) การกำหนดขอบเขตและแนวทางในการบริหารจัดการโครงการ (Project Management) ที่สนองตอบความต้องการของการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัลในระดับองค์กร โดยครอบคลุมถึง

- การบริหารจัดการแผนงานและโครงการ (Programmed and Projects)
- การบริหารจัดการข้อกำหนดและความต้องการ (Requirements Definition)
- การบริหารจัดการการระบุและการจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ (Solutions Identification and Build)
- การบริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล (Organizational Change Enablement)
- การบริหารจัดการการเปลี่ยนแปลง (Changes)
- การบริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน (Change Acceptance and Transitioning)

รัฐวิสาหกิจมีการสื่อสารแนวทางสำหรับการบริหารจัดการโครงการ (Project Management Skills (Knowledge areas) Communications)
การกำหนดแนวทางการประเมินความสำเร็จของโครงการด้านดิจิทัลที่บรรลุเป้าหมาย/ผลลัพธ์ตามที่กำหนดไว้
การจัดทำแผนบริหารความเสี่ยงของโครงการ (Project Risk Management Plan)
มีการกำหนดเกณฑ์การวัดประสิทธิภาพของโครงการ (Project performance criteria)
การกำหนดแนวทางในการทบทวนหลังจากการดำเนินงานโครงการ (Post-implementation review)

รัฐวิสาหกิจมีกระบวนการบริหารจัดการโครงการ และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ มีการถ่ายทอดกระบวนการบริหารจัดการโครงการ
แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการโครงการ
และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน

การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว)
มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล ซึ่งประกอบด้วย

- การบริหารจัดการข้อกำหนด และความต้องการ
- การบริหารจัดการการระบุ และการจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ
- การบริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล
- การบริหารจัดการการเปลี่ยนแปลง
- การบริหารจัดการการยอมรับการเปลี่ยนแปลง และการปรับเปลี่ยน
-

การกำหนดแนวทางการประเมินความสำเร็จของโครงการด้านดิจิทัลที่บรรลุเป้าหมาย/ผลลัพธ์ตามที่กำหนดไว้

- การจัดทำแผนบริหารความเสี่ยงของโครงการ
- การกำหนดเกณฑ์การวัดประสิทธิภาพของโครงการ
- การกำหนดแนวทางในการทบทวนหลังจากการดำเนินงานโครงการ

การดำเนินงานโครงการ (Project Execution) เป็นการดำเนินการตามแผนการปฏิบัติงานโดยผู้จัดการโครงการจะเป็นผู้รับผิดชอบสายงานหลัก
และควบคุมกำกับดูแลให้การดำเนินการโครงการเป็นไปตามวัตถุประสงค์ เป้าหมาย ผลผลิตผลลัพธ์ที่กำหนด

ภาพการดำเนินงานโครงการ (Project Execution)

การติดตามและการควบคุม (Monitoring and Control) เป็นเครื่องมือสำคัญของกระบวนการบริหารและกระบวนการวางแผน ทำให้การดำเนินการเป็นไปตามวัตถุประสงค์ นโยบายที่กำหนดไว้การติดตามและการควบคุมนั้น เป็นกิจกรรมทีเกี่ยวเนื่องกัน มักจะใช้ควบคู่กันไม่ได้มีการแยกกันอย่างอิสระ คือ เมื่อมีการติดตามดูผลการทำงานว่าเป็น อย่างไรแล้วก็ต้องมีการควบคุมเพื่อปรับปรุงปฏิบัติงานดังกล่าวให้ไปสู่ทิศทางที่ต้องการ และในทางกลับกันหน่วยงานใดก็ตามที่จะทำหน้าที่ควบคุมก็ต้องมีการติดตามก่อนเสมอ ไม่เช่นนั้นก็จะไม่สามารถควบคุมได้ ประโยชน์การติดตามและการควบคุม มีรายละเอียดดังนี้

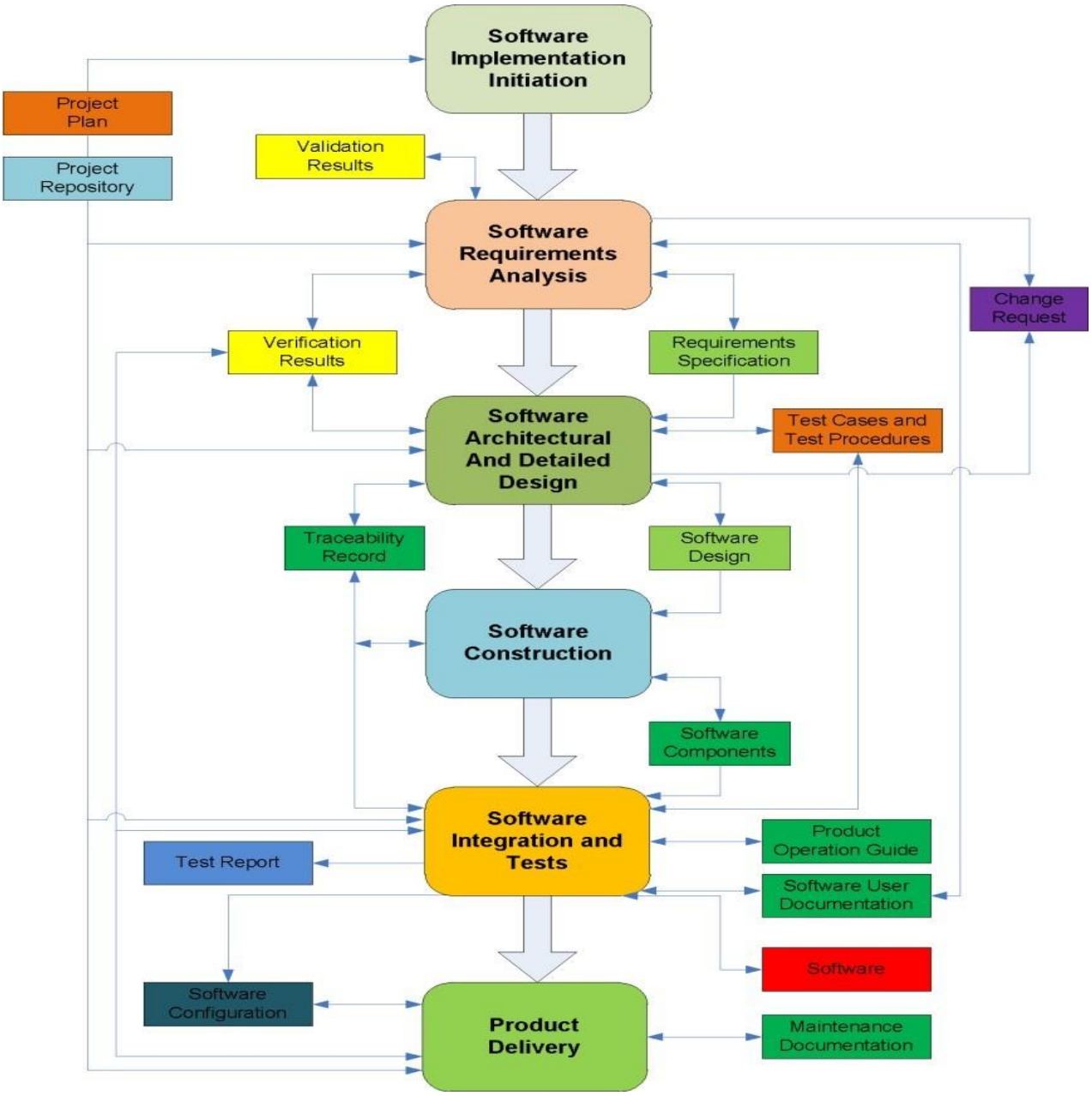
- เพื่อให้แผนบรรลุเป้าหมายและวัตถุประสงค์ที่ตั้งไว้ ถือเป็นหัวใจสำคัญของโครงการ หากไม่มีการยึดเป้าหมายและวัตถุประสงค์เป็นหลักแล้ว เราก็ไม่ทราบว่าจะทำโครงการนี้ไปทำไม เมื่อเป็นเช่นนี้ การติดตามและควบคุม การปฏิบัติงานต่างๆ ที่จะช่วยให้โครงการบรรลุสิ่งที่มุ่งหวังจึงถือเป็นกิจกรรมที่สำคัญของผู้บริหารโครงการ
- ช่วยประหยัดเวลาและค่าใช้จ่าย ผู้บริหารจะต้องควบคุมเวลาและค่าใช้จ่ายของโครงการโดยการเสนอแนะเทคนิควิธีการปฏิบัติที่มีประสิทธิภาพให้ซึ่งจะสามารถลดเวลาและค่าใช้จ่ายของโครงการลงไปได้มาก ทำให้ สามารถนำทรัพยากรที่ลดลงไปใช้ประโยชน์กับโครงการอื่น หรือเพื่อวัตถุประสงค์อื่นๆ ได้
- ช่วยกระตุ้น จูงใจ และสร้างขวัญกำลังใจให้ผู้ปฏิบัติงาน

การติดตามควบคุมนั้นไม่ใช่เป็นการจับสังเกตเพื่อ ลงโทษ
แต่เป็นการแนะนำช่วยเหลือโดยคำนึงถึงผลสำเร็จของโครงการเป็นสำคัญ เพราะฉะนั้น
ผู้นิเทศงานและผู้ควบคุม งานที่ดีมักจะได้รับการต้อนรับจากผู้ปฏิบัติงาน
ทำให้ผู้ปฏิบัติงานรู้สึกกระตือรือร้น เพราะมีพี่เลี้ยงมาช่วยแนะนำ ช่วยเหลือ
สร้างขวัญกำลังใจที่จะปฏิบัติงานต่อสู้กับปัญหาอุปสรรคต่างๆ ก็จะมีมากขึ้น

- ช่วยป้องกันและความเสียหายรุนแรงที่อาจจะเกิดขึ้นได้
  โครงการบางโครงการถ้ามีการควบคุมไม่ดีพออาจ เป็นสาเหตุให้เกิดความเสียหายใหญ่ได้
  และหากพบความเสียนั้นตั้งแต่ต้น ลักษณะของเหตุการณ์ที่เรียกว่า “สายเกินแก้” ก็ จะไม่เกิดขึ้น
- ทำให้พบปัญหาที่อาจเกิดขึ้น
  ทั้งนี้ในขณะที่ทำการติดตามและควบคุมนั้นผู้บริหารจะมองเห็นปัญหาอันเป็นผลกระทบต่างๆ
  ของโครงการหลายประการ จึงจะสามารถจัดหาแนวทางในการป้องกันแก้ไขได้อย่างถูกต้อง
- ช่วยให้ผู้เกี่ยวข้องทุกฝ่ายได้เห็นเป้าหมายวัตถุประสงค์หรือมาตรฐานของงานได้ชัดเจนขึ้น โดยปกติ
  โครงการ ต่างๆ มักจะกำหนดวัตถุประสงค์หรือเป้ามายไว้อย่างหลวมๆ
  หรือใช้คำที่ค่อนข้างจะเป็นนามธรรมสูง เช่น คำว่าพัฒนา ขยาย ปรับปรุง กระตุ้น ยกระดับ ฯลฯ
  ซึ่งทำให้ผู้ปฏิบัติงานไม่อาจปฏิบัติงานให้บรรลุเป้าหมายที่ถูกต้องได้ เมื่อมีการ
  ติดตามและควบคุมโครงการจะต้องมีการทำให้วัตถุประสงค์และเป้าหมายรวมทั้งมาตรฐานต่างๆ
  ชัดเจนขึ้น เพื่อจะได้ สามารถเปรียบเทียบและทำการควบคุมได้

4.2 Software Implementation (SI) Process เป็นกระบวนการ ที่ใช้ในการดำเนินงาน โดยอ้างอิงตามแผนที่ได้จาก Project Management Process ซึ่งจะเป็นแนวทางในการดำเนินงานทั้งในส่วนของการวิเคราะห์ความต้องการของระบบ การออกแบบระบบ การพัฒนาระบบงานตามที่ได้ออกแบบไว้ รวมถึงการทดสอบการใช้งาน และการส่งมอบงานให้ลูกค้า ไม่ว่าจะเป็นกระบวนการ PM หรือ SI ต่างก็ต้องมี Input Products และ Output Products ของแต่ละกิจกรรมที่ต้องดำเนินการ ในที่นี้จะเรียกรวมๆ ว่า Work Products ถ้าหากมองภาพง่ายๆ กว้างๆ Work Products ก็คือเอกสารที่เกี่ยวข้องของการดำเนินการในแต่ละกิจกรรม

Software Implementation Process ประกอบด้วย Activities (กิจกรรม) ทั้งสิ้น 6 Activities ได้แก่



1. Software Implementation Initiation เป็นการเริ่มต้นกระบวนการของ Software Implementation โดยน า กิจกรรมต่างๆ ที่ถูกวางแผนไว้ใน Project Plan ให้ผู้ที่เกี่ยวข้องได้รับทราบโดยทั่วถึง

2. Software Requirements Analysis เป็นกระบวนการวิเคราะห์ความต้องการของระบบที่จะได้จากลูกค้า อันจะได้มาซึ่ง Requirement Specification ที่จะต้องให้ลูกค้าตรวจสอบและยืนยันความถูกต้องของความต้องการนั้นๆ ก่อนที่จะน า Requirement Specification ที่ได้รับการยืนยันจากลูกค้า ไปเป็นตัวตั้งในกิจกรรมต่อๆ ไป

3. Software Architectural and Detailed Design เป็นกระบวนการแปลงความต้องการของลูกค้าไปเป็นระบบงาน โดยเป็นการวิเคราะห์และออกแบบระบบเพื่อให้ตอบโจทย์ตาม Requirement Specification

ที่ได้รับการยืนยันจากลูกค้าแล้ว

4. Software Construction เป็นการบวนการในการลงมือพัฒนาระบบ เป็นช่วงของการเขียน โปรแกรม โดยอ้างอิงตาม Software Design ที่ได้มาจากกิจกรรมก่อนหน้า

5. Software Integration and Tests เป็นกระบวนการในการทดสอบระบบ หลังจากที่ได้พัฒนาเสร็จแล้ว เพื่อให้แน่ใจว่า เป็นไปตามความต้องการของลูกค้า ก่อนที่จะน าไปส่งมอบและติดตั้งให้ลูกค้าใช้งาน กระบวนการการพัฒนาซอฟต์แวร์ตามมาตรฐานสากล

6. Product Delivery เป็นกระบวนการส่งมอบงานให้กับลูกค้า โดยอ้างอิงตามสิ่งที่ต้องส่ง ตามที่ได้ระบุไว้ใน Project Plan ซึ่งรวมถึงระบบงานที่ได้พัฒนาและผ่านกี่ทดสอบแล้ว

ตัวอย่างแผนงาน/โครงการ จากแผนปฏิบัติการดิจิทัล ประจำปี

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4			หมายเหตุ
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
5	รายงานโครงการตามแผนปฏิบัติงานประจำปี															
	5.1 แผนงาน/โครงการจัดหา	เสนอจัดซื้อ/จัดจ้างตามแผนงานงบลงทุน	วัดแผนงาน/โครงการและการบริหารโครงการ													
	1.รวบรวมข้อมูลระบบงาน (ศึกษาสำรวจความต้องการ)															
	2.เสนอจัดซื้อจ้างจ้าง															
	3.ทดสอบและอบรมการใช้งาน															
	4.รายงานผลประจำเดือนที่ประชุมผู้บริหาร															
	5.รายงานผลคณะอนุกรรมการฯ															

บทที่ 5

การบูรณาการเชื่อมโยงข้อมูลดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management)

5.1 การบูรณาการเชื่อมโยงข้อมูลดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)

การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) การออกแบบความเชื่อมโยงและการทำงานร่วมกัน (Enterprise Collaboration and Interoperability Design) กระบวนการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) กำหนดขอบเขตและแนวทางในการนำข้อมูลและการดำเนินการทั้งหมดที่ได้ออกแบบกิจกรรม กระบวนการ ทรัพยากร ให้มีความชัดเจนเกี่ยวกับการเชื่อมโยง และการทำงานร่วมกัน ทั้งระบบเทคโนโลยีดิจิทัล โครงสร้างสถาปัตยกรรม กระบวนการ ข้อมูล และตารางวัดผล โดยเป็นการเชื่อมโยงกับกระบวนการต่างๆ กำหนดแนวทางการเลือกคู่ความร่วมมืออย่างเป็นรูปธรรม (Partner Selection) กำหนดแนวทางปฏิบัติ/แผนงานที่เกี่ยวกับการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันอย่างเป็นรูปธรรม

ตามแผนปฏิบัติงานประจำปีกำหนดให้มีการทบทวนคู่มือการปฏิบัติงานด้านสถาปัตยกรรมองค์กร (Enterprise Architecture) ของรัฐวิสาหกิจ โดยการสำรวจหรือตามข้อเสนอแนะของที่ประชุมผู้บริหารในแต่ละเดือน และกำหนดแผนการปรับปรุงคู่มือปฏิบัติงานด้านเทคโนโลยีสารสนเทศ หรือ คู่มือ iT ควบคู่กันไปเพื่อให้การดำเนินงานสอดคล้องกันอย่างเป็นระบบและมีประสิทธิภาพ

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
	1.2 คู่มือปฏิบัติงานด้านเทคโนโลยีสารสนเทศ		เป็นไปตามขั้นตอน ผ่านการพิจารณาอย่างถูกต้องครบถ้วนจากคณะอนุกรรมการฯ และรายงานคณะกรรมการบริษัทฯ รับทราบภายในเวลาที่กำหนด												
	1.2.1 คณะทำงานการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล														
	1.2.2 คณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล														
	1.2.3 คณะกรรมการบริษัท อู่กรุงเทพ จำกัด														
	1.3 คู่มือสถาปัตยกรรมองค์กร														
	1.3.1 คณะทำงานการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล														
	1.3.2 คณะอนุกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล														
	1.3.3 คณะกรรมการบริษัท อู่กรุงเทพ จำกัด														

รัฐวิสาหกิจมีกระบวนการบูรณาการการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงานและแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย

- การกำหนดข้อมูลขององค์กรที่สามารถเปิดเผย จัดประเภทข้อมูล/สารสนเทศขององค์กร แลกเปลี่ยนข้อมูล/เปิดเผยข้อมูลกับหน่วยงานอื่น กำหนดช่องทางการเข้าถึงข้อมูล รวมถึงการสำรวจความพึงพอใจต่อการเข้าถึงข้อมูลและสารสนเทศ
- รัฐวิสาหกิจกำหนดแนวทางการเลือกคู่ความร่วมมืออย่างเป็นรูปธรรม (Partner Selection)
- การกำหนดนโยบาย/แนวทางส่งเสริมการทำงานร่วมกันระหว่างหน่วยงานพัฒนาระบบการทำงานร่วมกันระหว่างหน่วยงานภาครัฐ ทบทวนแผนงาน/โครงการที่มีความซ้ำซ้อนกันในทุกระดับ เพื่อวางแผนบูรณาการการทำงานร่วมกัน โดยกำหนดเป็นแผนปฏิบัติการขององค์กรที่ชัดเจนเป็นรูปธรรม
- แผนปฏิบัติการขององค์กรที่เกี่ยวกับการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกัน
- มีการถ่ายทอดกระบวนการบูรณาการการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน

การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว)
มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

5.2 การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management)

รัฐวิสาหกิจมีการดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ที่ครอบคลุมถึงกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร ซึ่งประกอบด้วย

- กระบวนการกำกับดูแลข้อมูลที่เป็นมาตรฐานหน่วยงาน
- โครงสร้างการกำกับดูแลข้อมูลที่ชัดเจน
  มีส่วนงานกลางในการกำกับดูแลซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและไอที
- นโยบายข้อมูลและการตรวจสอบบังคับใช้ทั้งหน่วยงาน
- การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล
- การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
- กระบวนการกำกับดูแลข้อมูล
- โครงสร้างการกำกับดูแลข้อมูล
- นโยบายข้อมูลและการตรวจสอบ
- การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล
- การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
- การกำหนดข้อมูลและสารสนเทศที่สำคัญขององค์กร
- การกำหนดสิทธิ หน้าที่
  และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน
  เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้อง แม่นยำ ครบถ้วน เป็นปัจจุบัน และใช้งานง่าย
- มีการถ่ายทอดกระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร
  แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
  โดยมีการแสดงการวิเคราะห์ที่ชัดเจน
  และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของ
  กระบวนการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร

และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน
การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว)
มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

ตามแผนปฏิบัติงานประจำปี

กำหนดให้มีการติดตามสนับสนุนการใช้งานของแต่ละหน่วยงานในองค์กรเพื่อกำกับดูแลข้อมูลสารสนเทศขององค์กรอย่างมีระบบและรวมศูนย์ในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ เช่น การจัดทำระบบอินทราเนทเพื่อรวบรวมข้อมูลเป็น DataCenter สำหรับเชื่อมโยงข้อมูลแต่ละหน่วยงานอย่างมีประสิทธิภาพในการคนหาและนำไปใช้เพื่อประโยชน์ต่อองค์กร และเป็นพื้นฐานสำคัญในการพัฒนานวตกรรมและการจัดการความรู้ขององค์กรต่อไป

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4			หมายเหตุ	หมายเหตุ
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.		
2	**การบริหารจัดการสารสนเทศ การพัฒนาเทคโนโลยีดิจิทัล**																
	2.1 ระบบสารสนเทศสนับสนุนการบริหารจัดการรัฐวิสาหกิจ	ระบบ EIS	มีการติดตามและรายงานผลการดำเนินงานต่อผู้บริหารและคณะอนุกรรมการ เพื่อเสนอคณะกรรมการบริษัทเพื่อทราบ													มีการใช้งานอย่างต่อเนื่องและมีประสิทธิภาพภายใต้แนวปฏิบัติสถาปัตยกรรมองค์กร และแผนปฏิบัติการดิจิทัลฯ	
	2.2 ระบบสารสนเทศที่สนับสนุนการบริหารความเสี่ยงและควบคุมภายใน	ระบบ RMS															
	2.3 ระบบสารสนเทศสนับสนุนการตรวจสอบภายใน	สนับสนุน ITA															
	2.4 ระบบสารสนเทศสนับสนุนการบริหารทรัพยากรบุคคล	ติดตาม HRM															
	2.5 ระบบสารสนเทศสนับสนุนกองปฏิบัติการ	ติดตาม MRP / ERP															
	2.6 ระบบสารสนเทศตอบสนองความต้องการผู้มีส่วนได้เสียภายนอก																
	- ปรับปรุงเว็บไซต์บริษัทฯ	พัฒนา Website by Joo															
	- พัฒนา Application รองรับการติดตามงานซ่อมทำ	เผยแพร่ ตามมาตรา 7 แ															
	2.7 ระบบสารสนเทศตอบสนองความต้องการผู้มีส่วนได้เสียภายใน	พัฒนาระบบอินทราเนท															

บทที่ 6
การบริหารจัดการ ความมั่งคงปลอดภัยสารสนเทศ
(Information Security Management)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) หรือ ระบบ ISMS หมายถึง
การบริหารจัดการความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศ ขององค์กร การกำหนดมาตรการเพื่อลด เพื่อป้องกัน หรือจัดการความเสี่ยง การดำเนินการตามมาตรการที่กำหนดไว้ การเฝ้าระวัง (เพื่อตรวจสอบปัญหาที่เกี่ยวข้อง) การทบทวน การรักษา
และปรับปรุงความมั่นคงปลอดภัยสำหรับทรัพย์สินสารสนเทศ ให้ดียิ่งขึ้น โดยการดำเนินการภายใต้ระบบ ISMS นี้มีจุดประสงค์เพื่อให้สอดคล้องกับการปฏิบัติตามมาตรฐาน ISO/IEC 27001:2005 ความมั่นคงปลอดภัย หมายถึง การสร้างหรือการรักษาความมั่นคงปลอดภัยให้กับทรัพย์สินสารสนเทศที่องค์กรดูแลและ รับผิดชอบ ทั้งนี้เพื่อป้องกันการสูญเสีย การสูญหาย การถูกขโมย การเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยโดยไม่ได้รับอนุญาต การปลอมแปลง การปฏิเสธความรับผิดชอบ หรือการกระทำใดๆ
ก็ตามที่ก่อให้เกิดความเสียหายต่อองค์ประกอบ ทางด้านความมั่นคงปลอดภัย 3 ส่วน ดังนี้

- ความลับ (Confidentiality) กล่าวคือ
  ทรัพย์สินสารสนเทศจะต้องสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตแล้วเท่านั้น
- ความถูกต้อง (Integrity) กล่าวคือ ทรัพย์สินสารสนเทศจะต้องมีความถูกต้องและสมบูรณ์ การเปลี่ยนแปลง สามารถทำได้ แต่ต้องโดยผู้ที่ได้รับอนุญาตแล้วเท่านั้น
- ความพร้อมใช้ (Availability) กล่าวคือ
  ทรัพย์สินสารสนเทศจะต้องมีสภาพความพร้อมใช้อยู่เสมอหรือสามารถ
  เข้าถึงได้เมื่อมีความจำเป็นต้องใช้งาน นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) หมายถึง แนวทางการปฏิบัติตามระบบบริหาร
  จัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001: 2005
  ที่ให้องค์กรได้ยึดเป็นแนวทางการดำเนินการ
  หรือประยุกต์เข้ากับการดำเนินงานทางเทคโนโลยีสารสนเทศขององค์กร
- การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the organization and its context) องค์กรต้องกำหนดประเด็นที่เป็นปัจจัยภายในและภายนอกที่เกี่ยวข้องกับจุดประสงค์ขององค์กรและที่จะส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) องค์กรต้องกำหนด

ผู้ที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
และความต้องการของผู้ที่เกี่ยวข้องเหล่านั้น
ข้อใดของความต้องการเหล่านี้ที่จะมีการดำเนินการผ่านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system)
  องค์กรต้องกำหนดขอบเขตและการประยุกต์ใช้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเพื่อระบุขอบเขตของการดำเนินงาน ในการระบุขอบเขต องค์กรต้องพิจารณาประเด็นที่เป็นปัจจัยภายในและภายนอกขององค์กร
  และความเชื่อมโยงและความสัมพันธ์กันของกิจกรรมในลักษณะที่กิจกรรมหนึ่งขึ้นอยู่กับอีกกิจกรรมหนึ่ง โดยที่กิจกรรมเหล่านั้นอาจดำเนินการโดยองค์กรเอง หรือโดยองค์กรอื่นๆ
  ขอบเขตต้องมีพร้อมไว้เป็นลายลักษณ์อักษรให้สามารถใช้งานได้

6.1 การบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร (Information Security Management)

กระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ (Information Security Management) ของรัฐวิสาหกิจ
มีการกำหนดนโยบายหรือแผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศครอบคลุมประเด็น ดังนี้

- การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)
- การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information security)
- การควบคุมการเข้าถึง (Access control)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
- การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)
- การรักษาความมั่งคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)
- การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System acquisition and development)
- การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT incident and problem management)
- การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
- การบริหารจัดการผู้ให้บริการภายนอก (Third party management)
- การป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention)
- การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท (Website and Internet Security)

- การรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint Security)
- การบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศ (Cryptography) และการบริหารจัดการกุญแจ (Key management)

รัฐวิสาหกิจมีการสื่อสารนโยบายหรือแผนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กร

มีการกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) ขององค์กร

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
4	**การบำรุงรักษาและบริหารจัดการเครือข่าย**														
	4.1 ตรวจสอบความพร้อมอุปกรณ์เครื่องแม่ข่าย Server	จัดทำแผนการตรวจสอบในประเด็นต่าง ๆ เช่น ทรัพย์สินความปลอดภัยข้อมูลการและการเข้าถึงการใช้งานด้านอุปกรณ์และความปลอดภัยจากสิ่งแปลกปลอมต่าง ๆ	ดำเนินการตรวจสอบการใช้งาน Server และอุปกรณ์เครื่องลูกข่ายของแต่ละหน่วยงาน ตามแผนงานประจำปี						⟷						
	4.2 ตรวจสอบระบบสนับสนุนเครือข่าย เช่น Antivirus / Firewall			⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷
	4.3 ตรวจสอบความพร้อมอุปกรณ์เครื่องลูกข่าย Client														
	- หน่วยงานตรวจสอบภายใน			⟷						⟷					
	- หน่วยงานประกันคุณภาพและความปลอดภัย				⟷						⟷				
	- กองบริหารทรัพยากร					⟷						⟷			
	- กองแผนงานการเงินและงบประมาณ						⟷						⟷		
	- กองธุรกิจและการตลาด							⟷						⟷	
	- กองปฏิบัติการ								⟷						⟷
	- หน่วยธุรกิจสัตหีบ				⟷						⟷				

รัฐวิสาหกิจมีการถ่ายทอดกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศแก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ

เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม

โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

6.2 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร

กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) มีการกำหนดปัจจัยภายในและภายนอกที่สอดคล้องกับวัตถุประสงค์และบริบทขององค์กร ซึ่งส่งผลต่อความสามารถในการบรรลุผลลัพธ์ตามที่ต้องการของการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร
มีนโยบายหรือแผนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
โดยอย่างน้อยประกอบด้วยหลักเกณฑ์ ระเบียบวิธีปฏิบัติ
และกระบวนการในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่

- การประเมินความเสี่ยง (Risk assessment) ประกอบด้วย
  - การระบุความเสี่ยง (Risk identification)
  - การวิเคราะห์ความเสี่ยง (Risk analysis)
  - การประเมินค่าความเสี่ยง (Risk evaluation)
- การจัดการความเสี่ยง (Risk treatment) เป็นแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- การติดตามและทบทวนความเสี่ยง (Risk monitoring and review) ควรมีการกำหนดผู้รับผิดชอบและจัดให้มีกระบวนการในการติดตามตัวชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามที่กำหนดและทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับที่ยอมรับได้
- การรายงานความเสี่ยง (Risk reporting) มีการนำเสนอผลการบริหารแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมกับการรายงานผลการประเมินและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศโดยเชื่อมโยงกับความเสี่ยงในระดับองค์กร

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กร คือ กระบวนการการทำงานที่ช่วยสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์ และการดำเนินธุรกิจ ระหว่างมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศ

และข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

- Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ เช่น มีการกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่เหมาะสมกับหน้าที่และความรับผิดชอบ และมีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่าง รัดกุมเพียงพอ เป็นต้น
- Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกบันทึก/แก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่เกี่ยวข้องกับ Aaccess risk ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงาน
- Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ เช่น มิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ หรือจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน
- Infrastructure Risk เป็นความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงาน ที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือรวมถึงการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การ สนับสนุนการดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

การประเมินความเสี่ยง (Risk assessment)

- การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสามารถแยกประเภทความเสี่ยงด้านเป็น 4 ประเภท ดังนี้

- ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะ ทำลายระบบจาก Cracker เป็นต้น
- ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่และอาจทำให้เกิดความ เสียหายต่อข้อมูลสารสนเทศได้
- ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
- ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
ความเสี่ยงในการเข้าถึง	ความเสี่ยงจาก	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้	- การอำพรางหรือสวมรอยผู้ใช้	ผู้ใช้งาน
ข้อมูลของบุคคลอื่น	ผู้ปฏิบัติงาน	ระบบสารสนเทศ เช่น การมอบหมายให้	/ การเข้าถึงข้อมูล - เปลี่ยนแปลง	
		ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบ	ข้อมูล โดยไม่ได้รับอนุญาต	ระบบสารสนเทศ
		หรือใช้งานแทน		ระบบฐานข้อมูล
ความเสี่ยงจากการนำเข้า	ความเสี่ยงจาก	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบ	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้า	ผู้ใช้งาน
อุปกรณ์อื่นที่ไม่ได้รับ	ผู้ปฏิบัติงาน	เครือข่าย เช่น การนำ wireless	ระบบ	ผู้ดูแลระบบ
อุปกรณ์อื่นที่ไม่ได้รับ	ผู้ปฏิบัติงาน	เครือข่าย เช่น การนำ wireless	ระบบ	ผู้ดูแลระบบ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
อนุญาตมาเชื่อมต่อ		หรือ switch/hub มาเชื่อมต่อกับระบบ	- ความล้มเหลวทางเทคนิค	
		เครือข่ายกรมโดยไม่ได้รับอนุญาต และ		ระบบสารสนเทศ
		ไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้		ระบบฐานข้อมูล
		เครื่องคอมพิวเตอร์อื่นในระบบเครือข่าย		เครื่องคอมพิวเตอร์แม่ข่าย
		ไม่สามารถใช้งานได้		
		หรือการไม่ได้ตั้งค่าการรักษาความ		
		ปลอดภัยทำให้เครื่องคอมพิวเตอร์ของ		
		บุคคลภายนอกอื่นๆที่รับสัญญาณได้		
		เชื่อมต่อเข้ากับระบบเครือข่ายของกรม		
		ทำให้เกิดช่องโหว่กับระบบรักษาความ		
		ปลอดภัยของกรม		

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
3. ความเสี่ยงจาก	ความเสี่ยงจากภัยหรือ	การเกิดกระแสไฟฟ้าขัดข้องหรือเกิด	- แหล่งกำเนิดไฟฟ้าขัดข้องหรือ	- ผใ้ ช้งาน

กระแสไฟฟ้าขัดข้อง	สถานการณ์ฉุกเฉิน	แรงดันไฟฟ้าไม่คงที่ทำให้เครื่อง	แรงดันไฟฟ้าไม่คงที่	- ผู้ดูแลระบบ
ไฟฟ้าดับ แรงดันไฟฟ้าไม่		คอมพิวเตอร์และอุปกรณ์อาจได้รับความ		- เครื่องคอมพวเตอร์แม่แม่ขาย
คงที่		เสียหายจากแรงดันไฟฟ้าที่ไม่คงที่		- อุปกรณ์เครือข่าย
		หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่อง		- เครื่องคอมพวเตอร์
		แม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่		- ระบบฐานข้อมูล
		สมบูรณ์ อาจทาให้ข้อมูลสารสนเทศ		- ระบบสารสนเทศ
		บางส่วนเกิดการสูญหาย และการ		
		ให้บริการบางประเภทไม่สามารถเปิดใช้		
		งานได้โดยอัตโนมัติ		

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
4. ความเสี่ยงจากการถูกบุกรุกโดยไม่ประสงค์ดี	ความเสี่ยงด้านเทคนิค /	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น	- แฮ็คเกอร์	- ผู้ใช้งาน
	ความเสี่ยงจากผู้ปฏิบัติงาน	hacker เป็นต้น การดักจับข้อมูล การส่ง	- แคร็กเกอร์	- ผู้ดูแลระบบ
		ข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือ	- การโจมตีการให้บริการ (denial	- คอมพิวเตอร์ Server

		เวิร์ม	of services/ DOS)	- ระบบฐานข้อมูล
			- การดักจับข้อมูล	- ระบบสารสนเทศ
			- คำสั่งเจตนาร้าย	
			- ความผิดพลาดของซอฟต์แวร์	
			หรือการเขียนโปรแกรม	
			- ไวรัส/เวิร์ม	

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่พิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- นโยบายจากรัฐบาล	-ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสาร

				สนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วยทำให้การดำเนินงานโครงการต่าง ๆ ได้รับผลกระทบ		-ผู้ใช้งาน -ผู้ดูแลระบบ -เครื่องคอมพิวเตอร์แม่ข่าย -อุปกรณ์เครือข่าย -ระบบฐานข้อมูล -ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินงานให้ระบบสารสนเทศสามารถดำเนินงานต่ออย่างมีประสิทธิภาพ		-ผู้ใช้งาน -ผู้ดูแลระบบ -เครื่องคอมพิวเตอร์แม่ข่าย -

				อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
8. ความเสี่ยงจากภัยภิบัติต่าง ๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดนไหวจนอาหารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ได้ทำให้ได้รับความเสียหายทั้งหมด	- ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ	-ผู้ใช้งาน -ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
9. ความเสี่ยงจาก	ความเสี่ยงจากภัยหรือ	การเกิดสถานการณ์ความรุนแรง หรือ	- การชุมนุมประท้วง	- ผู้ใช้งาน
สถานการณ์ความไม่สงบ	สถานการณ์ฉุกเฉิน	ความไม่สงบเรียบร้อย จนทำให้บุคลากร	- การจลาจล	- ผู้ดูแลระบบ

เรียบร้อยในบ้านเมือง		สามารถปฏิบัติงานได้ตามปกติ	- การก่อการราย	

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
10. ความเสี่ยงจากเครื่อง	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือ	- ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน
คอมพิวเตอร์หรืออุปกรณ์		ขัดข้องด้วยสาเหตุทางเทคนิคหรือจาก	- สัตว์กัดแทะประเภทหนู หรือ	- ผู้ดูแลระบบ
ขัดข้องไม่สามารถ		สัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	แมลง	- เครื่องคอมพวเตอร์แม่ข่าย
ทำงานได้ตามปกติ				- อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ
11. ความเสี่ยงจากการ	ความเสี่ยงด้านการ	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์	- การลักทรัพย์	- ผู้ใช้งาน
โจรกรรมเครื่อง	บริหารจัดการ/ความ	คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง		- ผู้ดูแลระบบ
คอมพิวเตอร์และอุปกรณ์	เสี่ยงจากผู้ปฏิบัติงาน	เช่น CPU และ Ram ทำให้ไมสามารถ		- เครื่องคอมพวเตอร์แม่ข่าย
		ปฏิบัติงาน หรือเกิดการสูญหายของข้อมูล		- อุปกรณ์เครอข่าย
		บนเครื่องคอมพิวเตอร์นั้นได้		

- การประมาณความเสี่ยง (Risk estimation) เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event)
  ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใดเกณฑ์การประมาณเป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับ โอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งกรมใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	5 ครั้ง/ป
4	สูง	4 ครั้ง/ป
3	ปานกลาง	3 ครั้ง/ ป
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี
ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสญเสียไมมาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคญั

- กระบวนการบำบัดความเสี่ยง (Risk treatment)

เมื่อผู้บริหารได้รับรายงานการประเมินความเสี่ยงแล้วจำเป็นต้องทำการตัดสินใจ โดยพิจารณาจากหลักเกณฑ์การยอมรับความเสี่ยงที่องค์กรมีอยู่ว่าจะยอมรับโดยไม่ทำอะไร หรือจะดำเนินการบำบัดความเสี่ยง ซึ่งได้แก่กระบวนการดังต่อไปนี้

- การยอมรับความเสี่ยง (acceptance) เป็นการยอมรับในความเสี่ยงโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวจริงเพียงใช้ id/ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การให้มีใช้ชีวมาตร (biometrics) เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่ คุ้มค่า
  โรงพยาบาลอาจยอมรับความเสี่ยงของระบบปัจจุบันและทำงานต่อไปโดยไม่ทำอะไร
- การเลี่ยงความเสี่ยง (avoidance) การหลีกเลี่ยงความเสี่ยง เช่น เมื่อพบว่าปัจจุบัน โรงพยาบาลมีการสำรองข้อมูลเพียง 1 ชุดและจัดเป็นความเสี่ยงต่อการสูญเสีย การเลี่ยงความเสี่ยงนี้อาจได้แก่การทำสำรองข้อมูล 2 ชุด และแยกเก็บในสถานที่ต่างกัน
  การบริหารจัดการการเชื่อมโยงสู่เครือข่าย
- ผ่านโมเด็ม ถ้าเป็นการยากต่อการควบคุมหรือบริหารจัดการ
  องค์กรอาจเลือกทางออกโดยการยกเลิกไม่ให้ ใช้บริการ และแนะนำให้พนักงานใช้บริการผ่านทาง ISP ในช่วงที่มีการระบาดของไวรัสอย่างหนัก องค์กร
  อาจมีเลือกระงับไม่ให้ใช้คอมพิวเตอร์ที่ไม่ได้ติดตั้ง Antivirus เป็นต้น
- การโอนยายความเสี่ยง (transfer) เช่น อุปกรณ์เครอข่ายเมื่อซื้อมาแล้วมีระยะประกัน
- การลดความเสี่ยง (reduction) ได้แก่การมีมาตรการควบคุมมากชนิดขึ้น หรือชนิดที่เข้มงวดมากขึ้นเพื่อลดความเสี่ยง เช่น การใช้ชีวมาตร (biometrics) เพื่อใช้ในการพิสจน์ตัวจริง
- การรายงานความเสี่ยงตกค้าง (Residual risk reporting)

เมื่อมีการบำบัดความเสี่ยงแล้ว จำเป็นต้องมีการรายงานและทบทวนอยู่เสมอเพื่อดูว่ามีการ ประเมินและการประเมินค่าความเสี่ยงอยู่ตลอดเวลา และดูว่ามาตรการควบคุมต่างๆที่ออกมาใช้ได้ผล หรือไม่เพียงไร วิธีการมาตรฐานที่ใช้กันโดยทั่วไป คือการมีหน่วยงานภายในหรือภายนอกทำการตรวจสอบ โดยกระบวนการ IT auditing ที่เหมาะสม เนื่องจากสิ่งแวดล้อมและกฎระเบียบมีพลวัตรและการ เปลี่ยนแปลงเกิดขึ้นตลอดเวลา จึงจำเป็นต้องมีการบริหารความเสี่ยงและการตรวจสอบเป็นประจำ

การเฝ้าสังเกต (Monitoring) กระบวนการเฝ้าสังเกตเป็นหลักประกันว่า องค์กรมีมาตรการต่างๆ ที่จำเป็นและเหมาะสมสำหรับ ได้มีการปฏิบัติตามมาตรการต่างๆและบังเกิดผล กระบวนงานที่กำหนดขึ้นมาสามารถปฏิบัติได้จริง มีการเรียนรู้เกิดขึ้นในหน่วยงานอันเป็นผลมาจากการบริหารความเสี่ยง

การสื่อสารนโยบายหรือแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร มีการกำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร การจัดทำ/ทบทวนขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร (Scope of Information Security Management System) นโยบายการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร (Information Security Management System Policy Statement) และคู่มือหรือแนวปฏิบัติการบริหารจัดการความมั่งคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร มีการถ่ายทอดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) มีการนำผลลัพธ์ที่สำคัญของกระบวนการเข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและ ทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

9.3 การตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร (Information Security Management System (ISMS) Audit)

กระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร (ISMS Audit) มีการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ (ISMS Audit) โดยมีแนวทางดังนี้

- วางแผน จัดตั้ง นำไปปฏิบัติ และรักษาให้คงไว้ตามแผนการตรวจประเมิน รวมถึงความถี่ วิธีการ หน้าที่ความรับผิดชอบ ข้อกำหนดของการวางแผนและการรายงานผล รวมทั้งให้ความสำคัญกับกระบวนการที่เกี่ยวข้องและผลการประเมินครั้งก่อน
- กำหนดเกณฑ์การตรวจประเมิน และขอบเขตการประเมินแต่ละครั้ง
- คัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินที่มีความเป็นกลางและความเป็นธรรม
- กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ (ISMS) ขององค์กร
- มีการถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน

โดยมีการแสดงการวิเคราะห์ที่ชัดเจน
และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม

- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome)
ของกระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร
และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน
การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว)
มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

ลำดับ	แผนงานกิจกรรม	แนวทางดำเนินการ	ตัวชี้วัด	ไตรมาส 1			ไตรมาส 2			ไตรมาส 3			ไตรมาส 4		
				ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
4	การบำรุงรักษาและบริหารจัดการเครือข่าย														
	4.1 ตรวจสอบความพร้อมอุปกรณ์เครื่องแม่ข่าย Server	จัดทำแผนการตรวจสอบในประเด็นต่าง ๆ เช่น ทรัพย์สินความปลอดภัยข้อมูลการและการเข้าถึงการใช้งานด้านอุปกรณ์และความปลอดภัยจากสิ่งแปลกปลอมต่าง ๆ	ดำเนินการตรวจสอบการใช้งาน Server และอุปกรณ์เครื่องลูกข่ายของแต่ละหน่วยงาน ตามแผนงานประจำปี						⟷						
	4.2 ตรวจสอบระบบสนับสนุนเครือข่าย เช่น Antivirus / Firewall			⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷	⟷
	4.3 ตรวจสอบความพร้อมอุปกรณ์เครื่องลูกข่าย Client														
	- หน่วยงานตรวจสอบภายใน			⟷						⟷					
	- หน่วยงานประกันคุณภาพและความปลอดภัย				⟷						⟷				
	- กองบริหารทรัพยากร					⟷						⟷			
	- กองแผนงานการเงินและงบประมาณ						⟷						⟷		
	- กองธุรกิจและการตลาด							⟷						⟷	
	- กองปฏิบัติการ								⟷						⟷
	- หน่วยธุรกิจสัตหีบ				⟷						⟷				

บทที่ 7
การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ
(Business Continuity and Availability Management)

7.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

กระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) รัฐวิสาหกิจกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและการเรียกคืนทรัพย์สิน

รัฐวิสาหกิจกำหนดผู้รับผิดชอบในการจัดทำ ปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศและบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมทั้งวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (End of life) หรือสิ้นสุดการใช้งาน (End of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

รัฐวิสาหกิจจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่รองรับระบบเทคโนโลยีสารสนเทศขององค์กรได้อย่างครบถ้วนและเป็นลายลักษณ์อักษร

- มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง
- มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (Return asset) เมื่อสิ้นสุดอายุการใช้งาน
- มีแนวทางในการบำรุงรักษาเชิงป้องกันสำหรับฮาร์ดแวร์ทั้งหมด (Preventive Maintenance Plan) หรือข้อตกลงในการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศกับหน่วยงานภายนอกที่ให้บริการ
- กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) ขององค์กร
- คู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) มีกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
    - การจัดทำทะเบียนรายการทรัพย์สิน
    - การปรับปรุงทะเบียนรายการทรัพย์สิน
    - การยกเลิกและการเรียกคืนทรัพย์สิน
    - การบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศ
    - การวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน

(end of life) หรือสิ้นสุดการใช้งาน (end of support)

- มีการถ่ายทอดกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและ ทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

7.2 การบริหารจัดการคอนฟิกูเรชั่น (Configuration Management)

กระบวนการบริหารจัดการคอนฟิกูเรชั่น (Configuration Management) ของรัฐวิสาหกิจ กำหนดขอบเขตและแนวทางในการบริหารจัดการคอนฟิกูเรชั่น (Configuration Management) การสอบทานการตั้งค่าจากหน่วยงานที่มีหน้าที่ควบคุมดูแลความปลอดภัยหรือความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของบริหารจัดการคอนฟิกูเรชั่น (Configuration Management) ขององค์กร

- การจัดทำคู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการบริหารจัดการคอนฟิกูเรชั่น (Configuration Management)
- มีกระบวนการบริหารจัดการคอนฟิกูเรชั่น และแนวปฏิบัติที่กำหนด อย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย การจัดทำ/ทบทวน minimum baseline standard การจัดเก็บการเปลี่ยนแปลงของการตั้งค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน (system configuration version control)
- มีการถ่ายทอดกระบวนการบริหารจัดการกำหนดค่า แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และ

มีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม

- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการคอนฟิกูเรชั่น และมีการนำผลลัพธ์ที่สำคัญของกระบวนการเข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

7.3 การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management)

กระบวนการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ของรัฐวิสาหกิจ*
มีการบริหารจัดการเหตุการณ์ผิดปกติ และการร้องขอการบริการด้านเทคโนโลยีสารสนเทศ (IT incident management and Service Requests) ซึ่งประกอบด้วย

- การกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการเหตุการณ์ผิดปกติและการร้องขอการบริการด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมกระบวนการหรือเครื่องมือในการบันทึกเหตุการณ์ผิดปกติและการร้องขอการบริการ การกำหนดประเภท การจัดระดับความรุนแรง การวิเคราะห์สาเหตุ การดำเนิน การแก้ไข การติดตามแก้ไข การรายงานเหตุการณ์ผิดปกติและการร้องขอการบริการ
- การกำหนดหลักเกณฑ์การส่งต่อเหตุการณ์ผิดปกติ (Escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหาร หรือคณะกรรมการ ได้รับทราบ
- การจัดลำดับความรุนแรงของปัญหา ควรครอบคลุมผลกระทบต่อการให้บริการ ผลกระทบต่อผู้ใช้งาน โดยกรอบระยะเวลาในการแก้ไขเหตุการณ์ผิดปกติและการร้องขอการบริการ ควรคำนึงถึงเป้าหมายระยะเวลาในการกู้คืน (Recovery Time Objective: RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption: MTPD)
- การมีศูนย์รับแจ้งเหตุการณ์ผิดปกติและการร้องขอการบริการ

โดยทำหน้าที่ในการบันทึกและแก้ไขในเบื้องต้นหรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

- จัดทำแผนการรับมือกับเหตุการณ์ผิดปกติและการร้องขอการบริการ (Incident and Service Request response plan) ตามความสำคัญของเหตุการณ์
  เพื่อให้สามารถรับมือและตอบสนองได้อย่างรวดเร็วและทันการณ์
  โดยแผนควรมีการระบุกระบวนการรับมือและช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก รวมทั้งมีแนวทางในการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ
- มีการจัดทำรายงานเหตุการณ์ผิดปกติและการร้องขอการบริการเสนอต่อผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมาย
- มีกระบวนการบริหารสภาวะวิกฤติ (Crisis management)
  เพื่อรองรับเหตุการณ์กรณีผิดปกติและการร้องขอการบริการด้านเทคโนโลยีสารสนเทศที่เพิ่มระดับความรุนแรงหรือมีความยืดเยื้อ

· รัฐวิสาหกิจมีการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ (IT Problem Management) ซึ่งประกอบด้วย

  - การกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการปัญหาด้านเทคโนโลยีสารสนเทศ
    เพื่อให้มีการนำเหตุการณ์ผิดปกติที่ยังไม่ทราบสาเหตุที่แท้จริง (Unknown root cause)
    เหตุการณ์ผิดปกติที่เกิดขึ้นซ้ำ (Repeated incident)
    มาวิเคราะห์และพิจารณาแนวทางแก้ไขปัญหาจากสาเหตุที่แท้จริง (Root cause)
  - กระบวนการหรือเครื่องมือในการบันทึกปัญหา หลักเกณฑ์ในการจัดประเภทปัญหา
    การจัดลำดับความสำคัญ วิเคราะห์ และจัดให้มีการติดตามแก้ไขปัญหา
    เพื่อให้ปัญหาได้รับการแก้ไข
  - กระบวนการหรือเครื่องมือบันทึกปัญหาที่เคยเกิดขึ้น
    เพื่อเป็นข้อมูลความรู้ให้สามารถสืบค้นเหตุการณ์ปัญหาและแนวทางแก้ไขในภายหลังให้รวดเร็วและมีประสิทธิภาพ

  รัฐวิสาหกิจมีการสื่อสารแนวการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ขององค์กร

กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) ขององค์กร

- มีคู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management)
- มีกระบวนการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ

และปัญหาด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย การแก้ไขปัญหาและกู้คืนความเสียหายที่เกิดขึ้นจาก Incident, Problems และ Service requests การสำรวจความพึงพอใจของผู้ที่มีส่วนเกี่ยวข้องกับ Incident หรือ Service requests

- มีการถ่ายทอดกระบวนการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ
  แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
  โดยมีการแสดงการวิเคราะห์ที่ชัดเจน
  และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome)
  ของกระบวนการบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ
  และปัญหาด้านเทคโนโลยีสารสนเทศ และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ
  เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล
  /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้
  และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
  โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

บทที่ 8
การบริหารจัดการความต่อเนื่องทางธุรกิจ
(Business Continuity Management)

กระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan) ของรัฐวิสาหกิจ มีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan) และ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan : DRP) ที่สอดคล้องกับนโยบายหรือแผนบริหารความต่อเนื่องทางธุรกิจและนโยบายการบริหารความเสี่ยงขององค์กร

- มีการจัดทำแผนและกำหนดเป้าหมายการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan)และ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan : DRP) ที่ได้รับอนุมัติจากคณะกรรมการบริหารความต่อเนื่องทางธุรกิจขององค์กร อย่างน้อยประกอบด้วย Maximum Tolerable Period of Disruption (MTPD)، Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)
- มีการสื่อสารแนวทางหรือแผนการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan) และ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan : DRP) ขององค์กร
- มีการดำเนินการทดสอบหรือซักซ้อมตามแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan) และ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan : DRP) ประจำปี
- กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Management) ขององค์กร
- มีกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับนโยบายหรือแผนบริหารความต่อเนื่องของธุรกิจและนโยบายการบริหารความเสี่ยงขององค์กร และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
    - การประเมินความเสี่ยง (risk analysis)
    - การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) ที่ครอบคลุมระบบงานที่สำคัญอย่างครบถ้วน (ทั้ง 8 เกณฑ์)
    - การจัดลำดับความสำคัญของระบบงาน
    - การกำหนดกลยุทธ์แผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
    - กำหนดเป้าหมายการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศที่สำคัญ อย่างน้อยประกอบดด้วย Maximum Tolerable Period of Disruption (MTPD)، Recovery Time

Objective (RTO) และ Recovery Point Objective (RPO)

- การจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การสื่อสารและฝึกอบรมแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- การทดสอบ ปรับปรุง
  และการสอบทานแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและ/หรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
- มีการถ่ายทอดกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจ
  แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
  โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของ
  ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน
  รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome)
  ของกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
  และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน
  การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว)
  มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและทำนวัตกรรม
  โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster Recovery Plan)

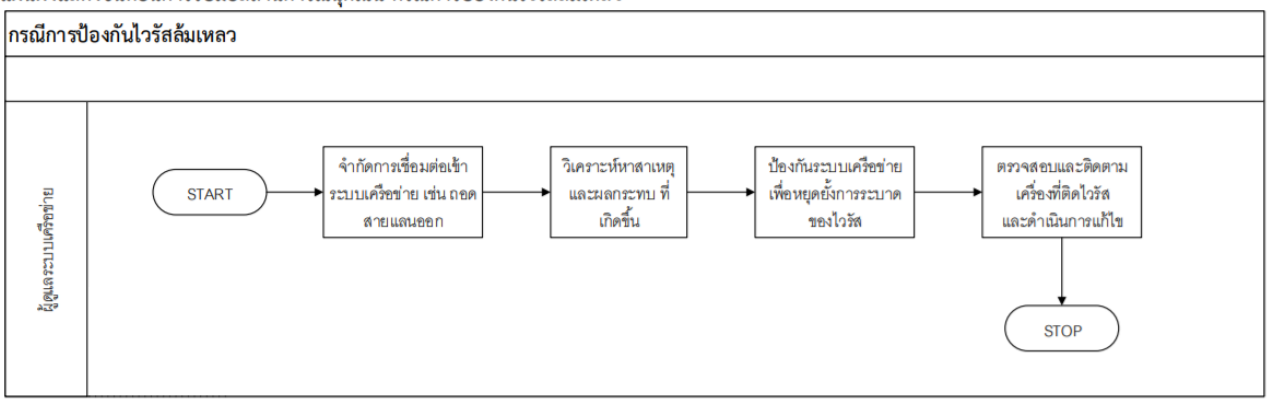
การนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีมาตราการการบริหารจัดการการเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการปฏิบัติงานอย่างเต็มประสิทธิภาพตลอดเวลา

8.1 กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก
  เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ ให้เจ้าหน้าที่งานพัฒนาระบบเครือข่ายและการสื่อสาร หรือที่ปรึกษากรณีมีเหตุอัน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว

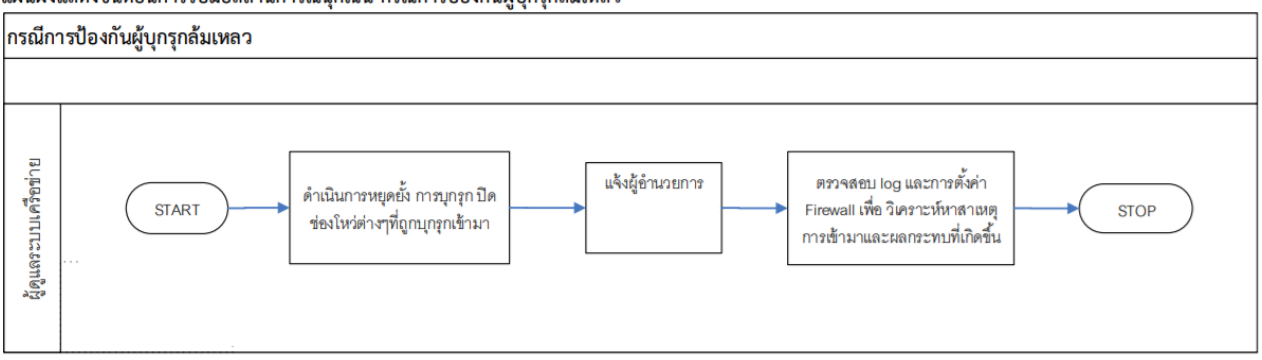


8.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก

  ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้นโดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งผู้อำนวยการแผนกเทคโนโลยีสารสนเทศให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุรุกเข้ามาได้
- ทาง บอท.ร่วมกับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในการเฝ้าระวัง

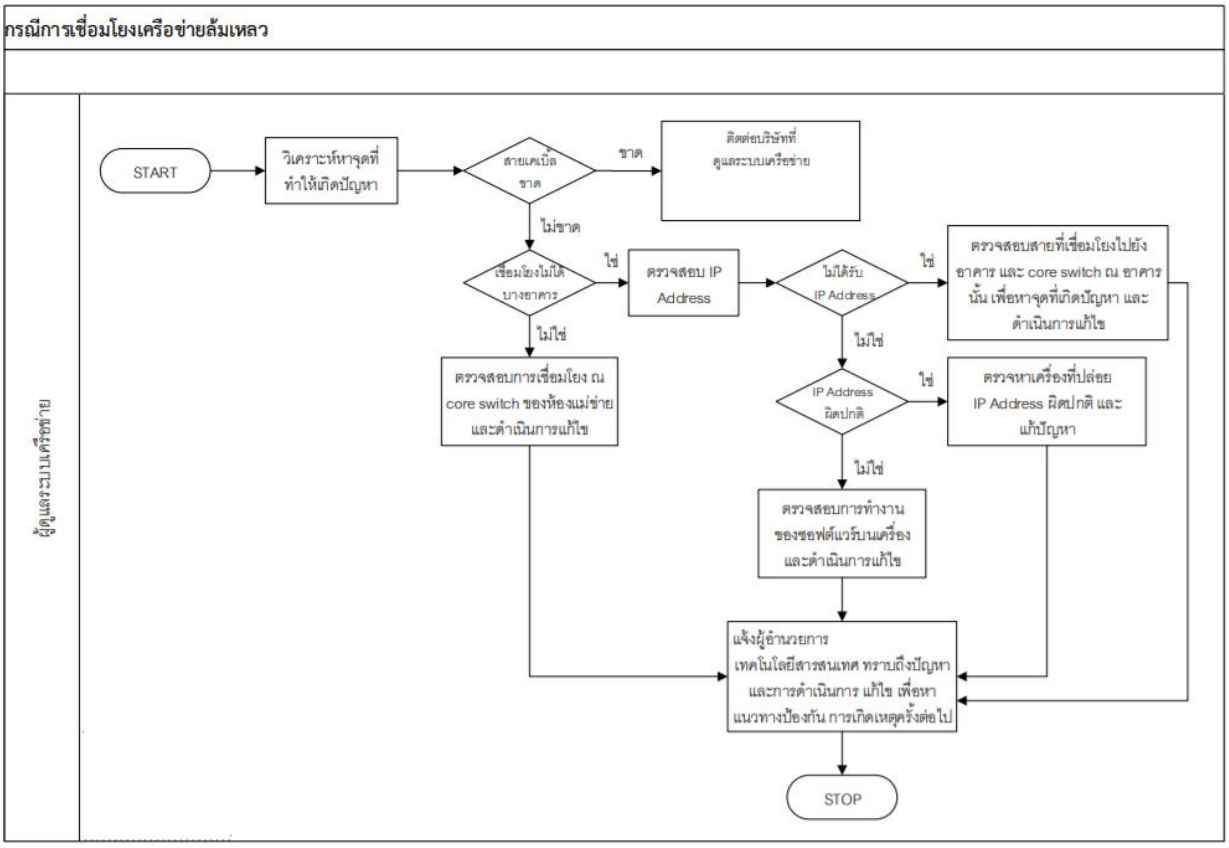
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



8.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลภายนอกขาด
  ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่ายมาดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคารหรือเป็นปัญหาภายในอาคาร
  ให้ดำเนินการตรวจสอบสายหรืออุปกรณ์ที่เชื่อมต่อและ core switch ที่ติดตั้งอยู่ในจุดที่ไม่สามารถเชื่อมต่อเครือข่ายได้

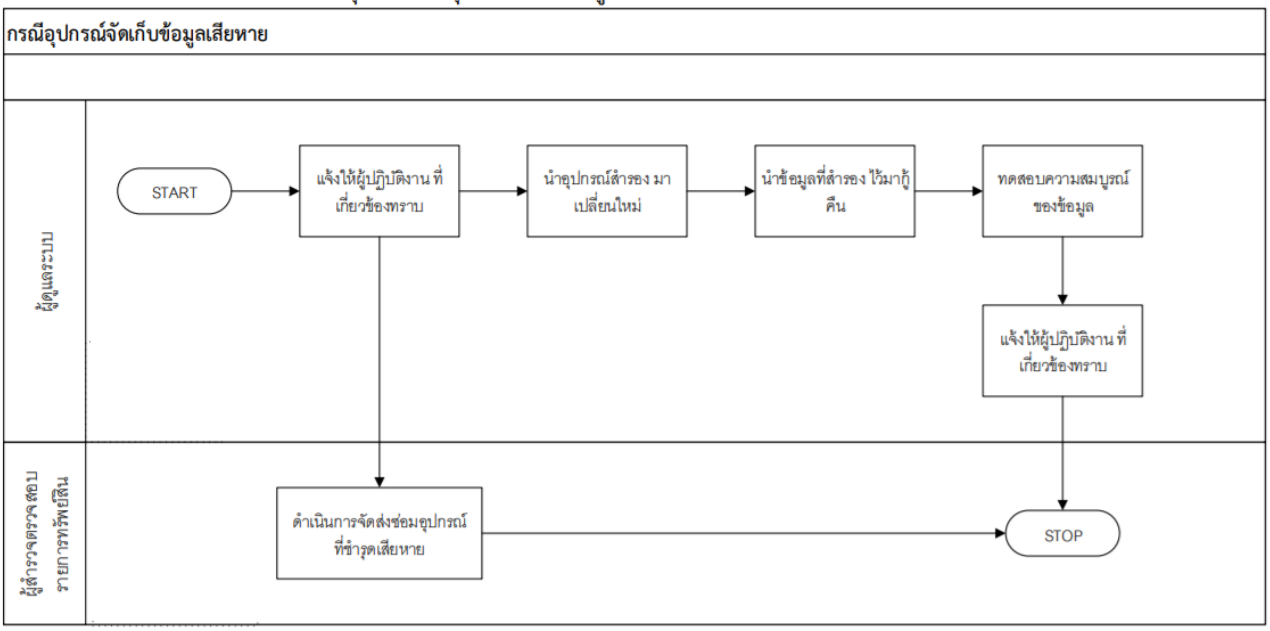
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



8.4 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



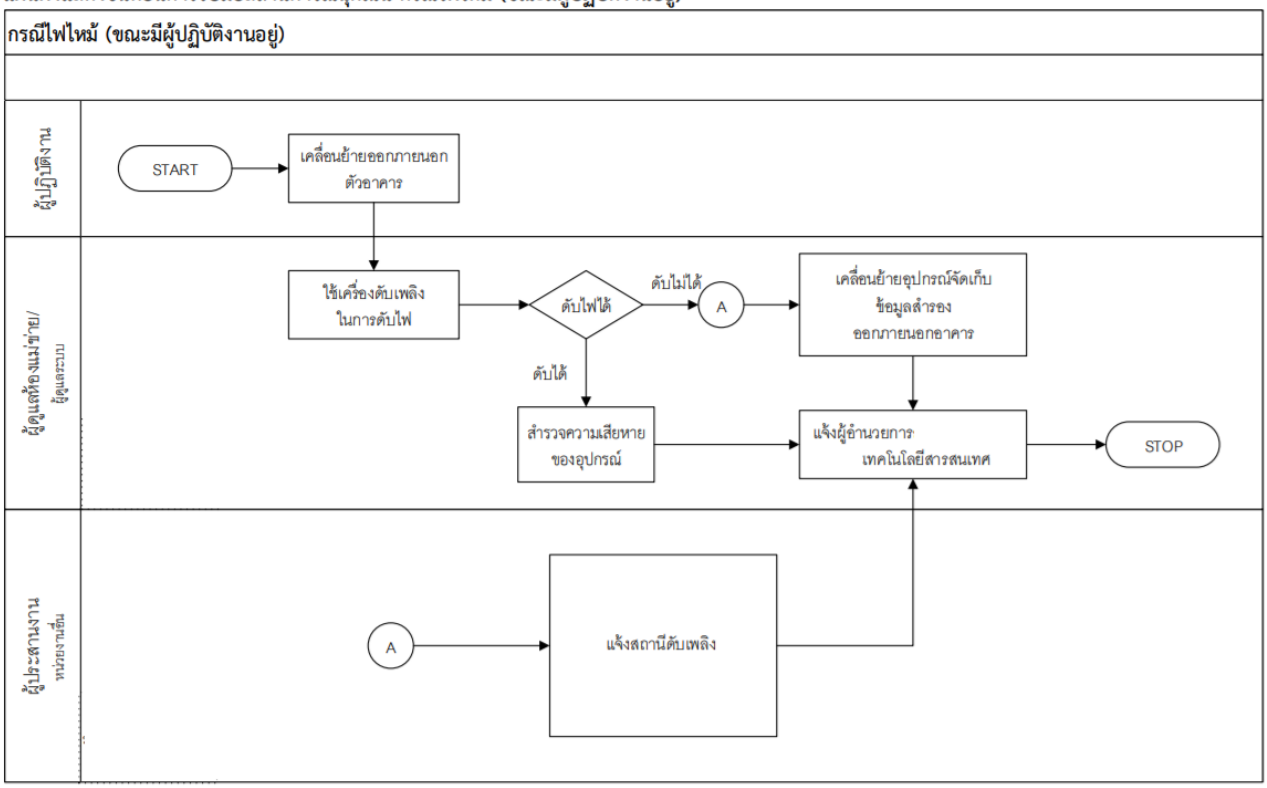
8.5 กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่
- ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้

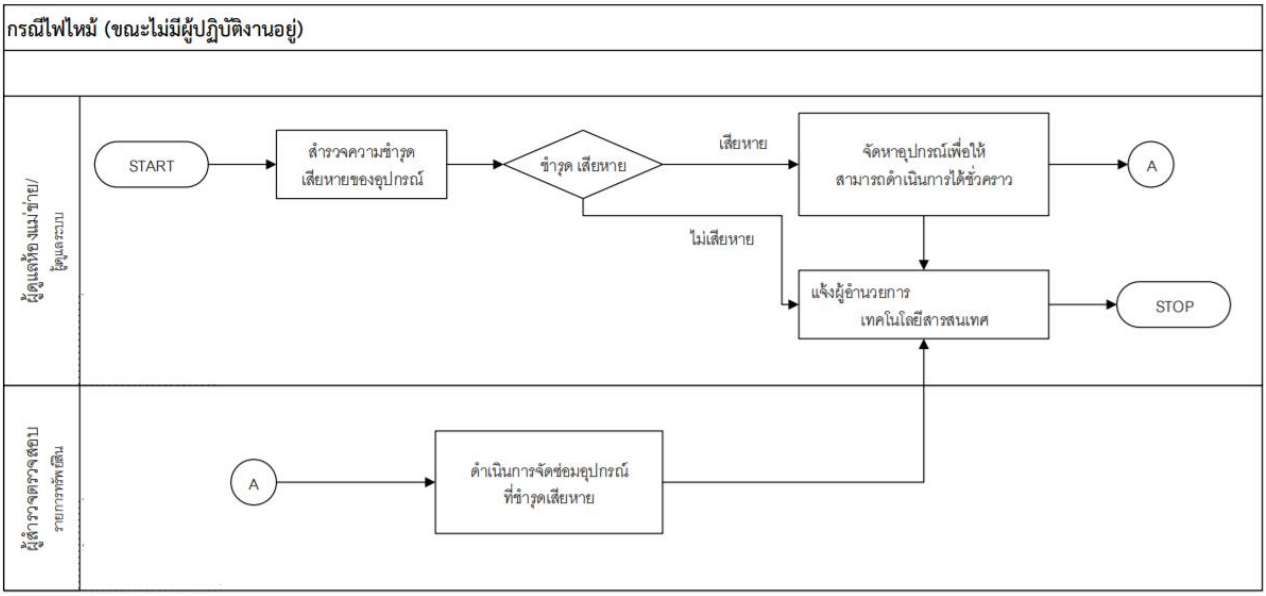
  ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร

  ผู้ติดต่อประสานงานโทรแจ้งหน่วยงานดับเพลิงและหน่วยงานที่เกี่ยวข้อง
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 2 ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)

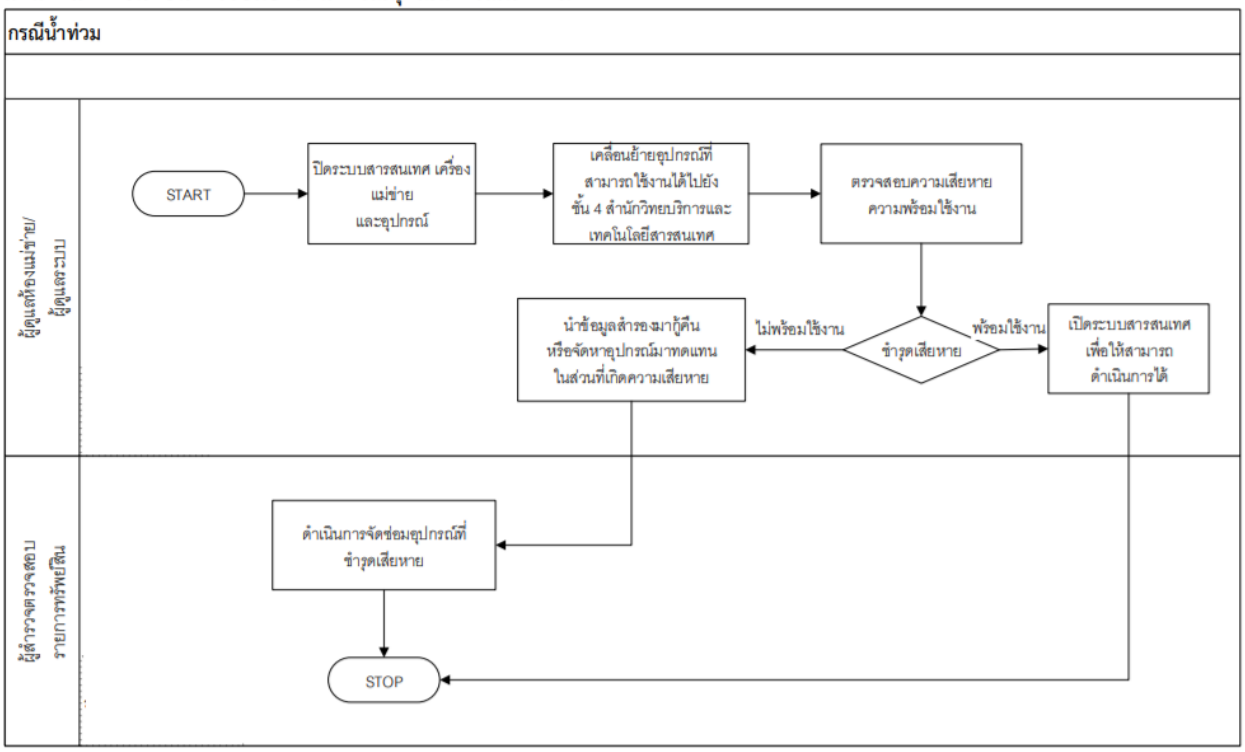


8.6 กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ สำนักงานสาขา

- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สินสำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

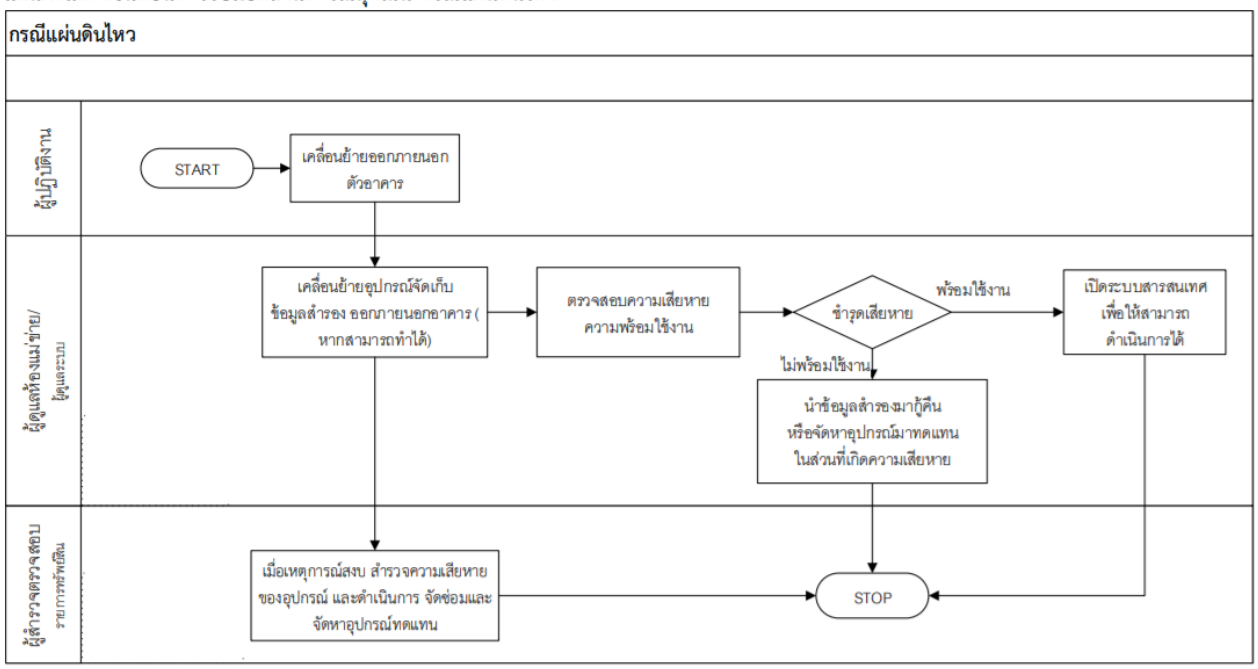
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



8.7 กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบน าข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

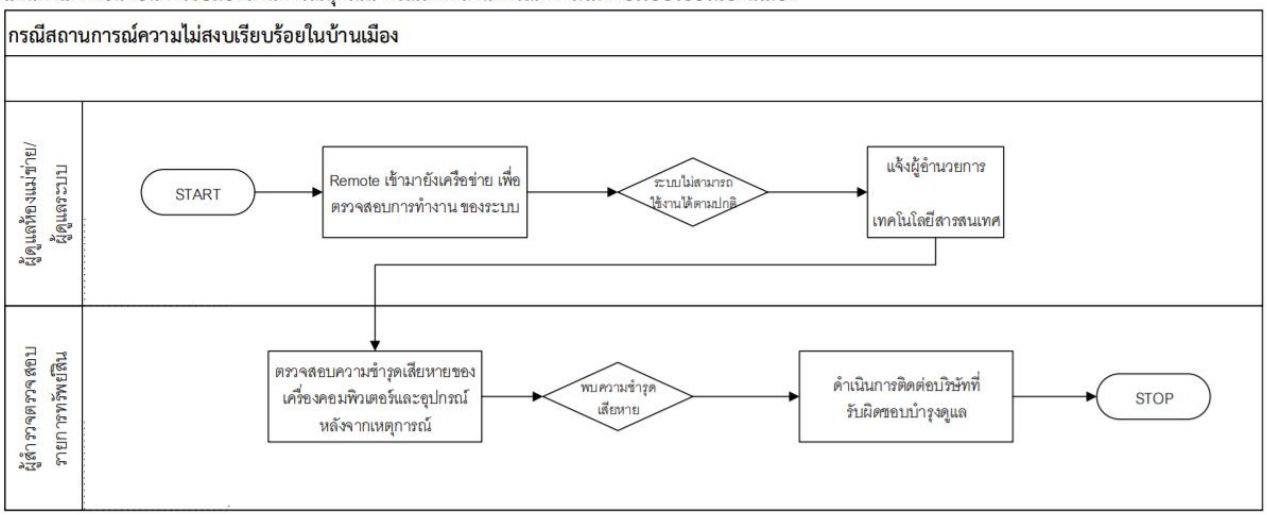
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



8.8 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติแจ้งผู้อำนวยการ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหายให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

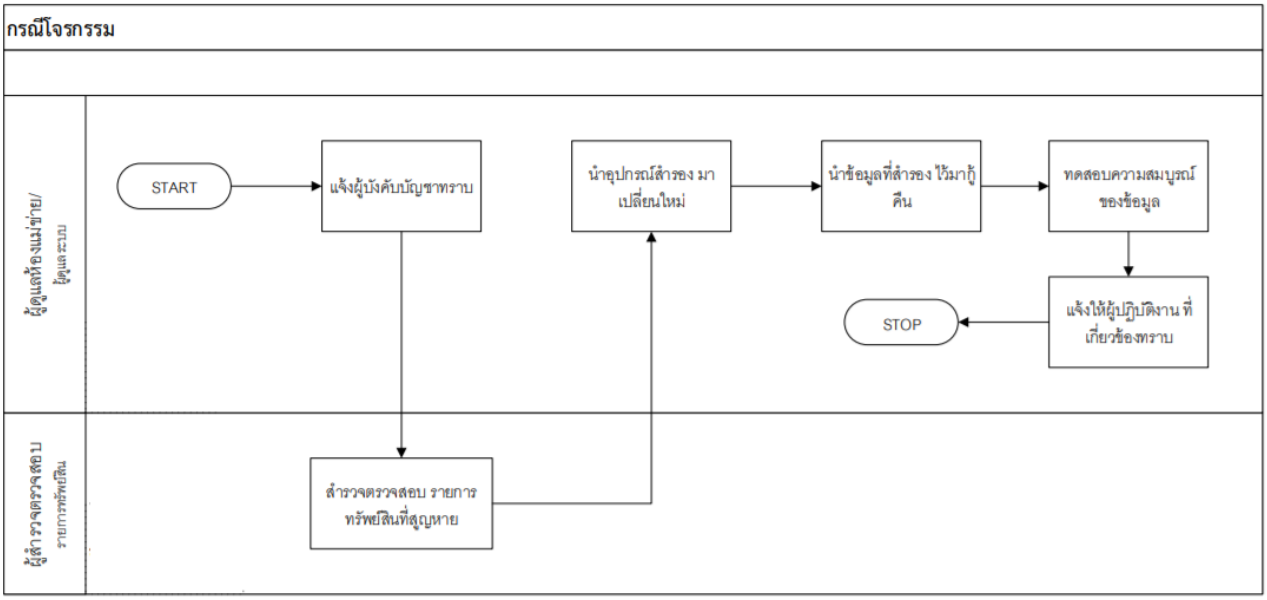
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



8.9 กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



บทที่ 9
การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม
(Resource Optimization Management)

9.1 การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management Implementation)

- กระบวนการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management Implementation) ของรัฐวิสาหกิจ*
- มีกรอบการจัดสรรงบประมาณ และกำกับให้การจัดสรร
  และใช้ทรัพยากรทั้งทางการเงินและไม่ใช่ทางการเงิน เป็นไปอย่างเพียงพอและมีประสิทธิภาพ
  รวมทั้งมีการประเมินความความเสี่ยง
- ด้านการจัดสรรทรัพยากร และมาตรการรองรับความเสี่ยงด้านการจัดสรรทรัพยากร
  ทุกโครงการที่สำคัญ
- มีนโยบายหรือแผนในการลดการใช้กระดาษและสาธารณูปโภคอื่นๆ
  เมื่อเทียบกับจำนวนพนักงานในองค์กร
- มีการสื่อสารแนวทางหรือแผนการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management) ขององค์กร
- กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่าง
- คู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management) ของรัฐวิสาหกิจ
- มีกระบวนการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม
  และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
  - การกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการจัดสรรทรัพยากรด้านเทคโนโลยีสารสนเทศ
  - การกำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการขีดความสามารถของเทคโนโลยีสารสนเทศ
  - การกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการกำหนดตัวชี้วัดและประเมินผลลัพธ์การใช้ทรัพยากรและการลงทุนด้านเทคโนโลยีสารสนเทศให้เกิดมูลค่าสูงสุด
  - การกำหนดตัวชี้วัดและประเมินผลลัพธ์การใช้ทรัพยากร ทางการเงิน การลงทุน และด้านอื่นๆ
    สำหรับการดำเนินโครงการ/แผนงาน/กิจกรรม
    ให้เป็นไปตามขั้นตอนและเป้าหมายที่กำหนดไว้ อย่างน้อยประกอบด้วย

ทรัพยากรทางการเงิน ทรัพยากรคน ระบบเทคโนโลยีดิจิทัล ระยะเวลา
ทรัพยากรพื้นฐานต่างๆ (เช่น อาคาร สถานที่ เป็นต้น)

- มีคู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management) ของรัฐวิสาหกิจ
- มีการถ่ายทอดกระบวนการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวนการกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้เพื่อนำไปปรับปรุงและทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

9.2 การบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT Management)

กระบวนการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT Management) ของรัฐวิสาหกิจ* มีนโยบายหรือมาตรการด้านการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT) ที่ให้ความสำคัญกับ 4 องค์ประกอบ ดังนี้

- วัฏจักรของอุปกรณ์ (Equipment Lifecycle) ประกอบด้วย การจัดซื้อ (Procurement) การรีไซเคิลและการนำกลับมาใช้ซ้ำ (Recycle & Reuse) การกำจัด (Disposal)
- การใช้ไอทีของผู้ใช้งาน (End User Computing) ประกอบด้วย คอมพิวเตอร์ส่วนบุคคล (Personal Computing) แบ่งเป็น Desktop และ Mobile คอมพิวเตอร์ในแต่ละหน่วยงาน (Departmental Computing) การพิมพ์และวัสดุสิ้นเปลือง (Printing and Consumables)
- ระบบประมวลผลข้อมูลขนาดใหญ่ในองค์กร (Enterprise Computing) ประกอบด้วย Data Center ICT Equipment, Data Center Environmental, Networking & Communications, Outsourcing & Cloud, Software Architecture
- การนำ ICT มาใช้ในการลดการปล่อยคาร์บอน (ICT as a Low – Carbon Enabler) ประกอบด้วย Governance & Compliance, Teleworking & Collaboration, Business Process Management, Business Applications, Carbon Emissions Management

รัฐวิสาหกิจมีการสื่อสารนโยบายหรือมาตรการด้านการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT) ขององค์กร
กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT) ขององค์กร

- มีคู่มือ/แนวทาง/นโยบาย/ระเบียบปฏิบัติ/ข้อกำหนดในการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT Management) ของรัฐวิสาหกิจ
- มีกระบวนการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม และแนวปฏิบัติที่กำหนดอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
    - วัฏจักรของอุปกรณ์ (Equipment Lifecycle)
    - การใช้ไอทีของผู้ใช้งาน (End User Computing)
    - ระบบประมวลผลข้อมูลขนาดใหญ่ในองค์กร (Enterprise Computing
    - การนำ ICT มาใช้ในการลดการปล่อยคาร์บอน (ICT as a Low – Carbon Enabler)
- มีการถ่ายทอดกระบวนการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม แก่ผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจน และมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการอย่างครบถ้วน รวมทั้งแสดงให้เห็นถึงแนวทางการนำกระบวนการไปปฏิบัติที่ชัดเจนเป็นรูปธรรม
- มีการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (outcome) ของกระบวนการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม และมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน การกำกับดูแลด้านการบริหารจัดการดิจิทัล /จัดทำแผนปฏิบัติการดิจิทัลขององค์กร (ระยะยาว) มีการนำผลที่ได้จากการประเมินไปเรียนรู้ และจัดการความรู้ เพื่อนำไปปรับปรุงและ ทำนวัตกรรม โดยมีการจัดเก็บความรู้และนวัตกรรมที่ได้ลงระบบดิจิทัล

บทที่ 10

คู่มือการปฏิบัติงาน (Procedure Manual)

10.1 วัตถุประสงค์

10.1.1 เพื่อให้ส่วนราชการมีการจัดคู่มือการปฏิบัติงานที่ชัดเจนอย่างเป็นลายลักษณ์อักษร ที่แสดงถึงรายละเอียดขั้นตอนการให้บริการของกิจกรรม/กระบวนการต่าง ๆ ของหน่วยงาน และสร้างมาตรฐานการปฏิบัติงานที่มุ่งไปสู่การบริการคุณภาพทั่วทั้งองค์กรอย่างมีประสิทธิภาพ เกิดผลงานที่ได้มาตรฐานเป็นไปตามเป้าหมายได้ผลิตผลหรือบริการที่มีคุณภาพและบรรลุข้อกำหนดที่สำคัญของกระบวนการ

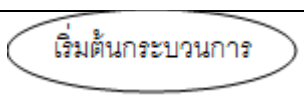
10.1.2 เพื่อเป็นหลักฐานแสดงวิธีการทำงานที่สามารถถ่ายทอดให้กับผู้เข้ามาปฏิบัติงานใหม่พัฒนาให้การทำงานเป็นมืออาชีพ และใช้ประกอบการประเมินผลการปฏิบัติงานของบุคลากร รวมทั้งแสดงหรือเผยแพร่ให้กับบุคคลภายนอกหรือผู้ใช้บริการให้สามารถเข้าใจและใช้ประโยชน์จากกระบวนการที่มีอยู่เพื่อขอการรับบริการที่ตรงกับความต้องการ

10.1.3 เพื่อให้การปฏิบัติงานการบริการด้านระบบคอมพิวเตอร์และเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นไปอย่างมีมาตรฐาน มีกำหนดระยะเวลาการให้บริการที่ชัดเจนและยกระดับการให้บริการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้มีประสิทธิภาพ และสามารถให้บริการได้ อย่างต่อเนื่อง

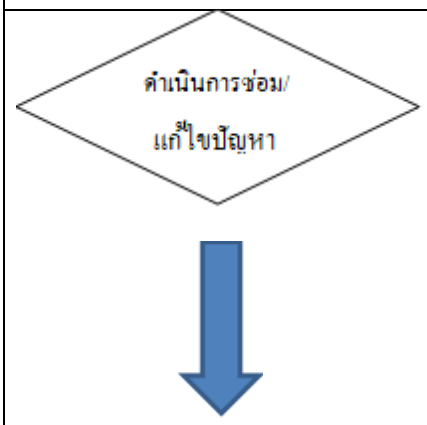
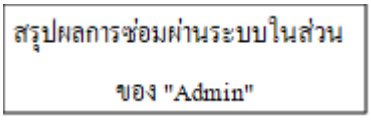
10.1.4 เพื่อให้หัวหน้าแผนกเทคโนโลยีสารสนเทศทำหน้าที่อนุมัติแผนการดำเนินงานพร้อมทั้งมอบหมายกำกับ ติดตามการปฏิบัติงานของผู้ที่ได้รับมอบหมาย เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศดำเนินงานตามคู่มือการปฏิบัติงาน Work Flow กระบวนงาน และขั้นตอนการปฏิบัติงาน

10.2 คู่มือการปฏิบัติงาน

10.2.1. งานบริการและซ่อมทำประจำวัน (Help Desk System)

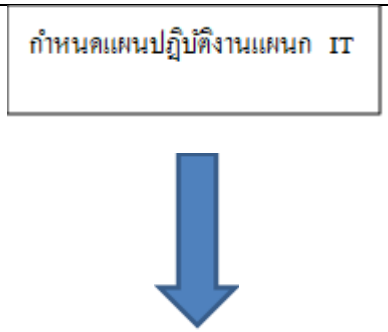
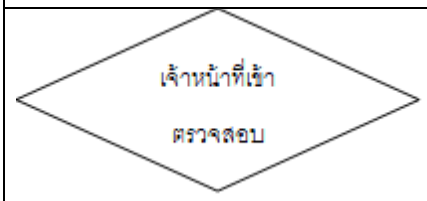
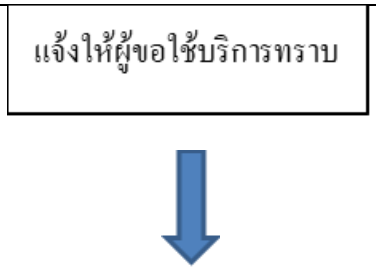
แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
	เข้าระบบแจ้งซ่อมคอมพิวเตอร์	หน่วยงานต้นสังกัด		

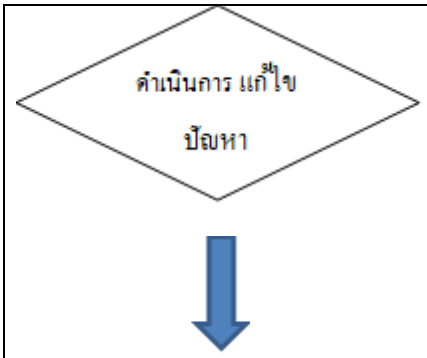
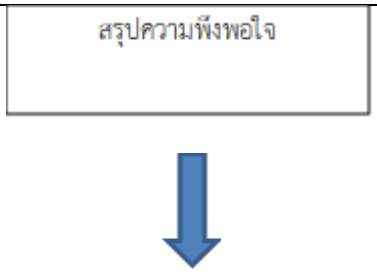
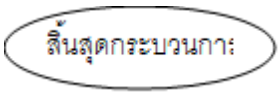
				
ผู้ใช้แจ้งซ่อมผ่านระบบ 	ผู้แจ้งซ่อมกรอกข้อมูลผ่านระบบให้ชัดเจน	หน่วยงานต้นสังกัด		http://www.bangkokdock.co.th/2556/helpdesk/index.php
เจ้าหน้าที่ตรวจสอบ 	ติดต่อผู้แจ้งซ่อม สอบถามปัญหาที่พบเบื้องต้น	พนักงาน IT	1วัน	
แจ้งให้ผู้ขอใช้บริการทราบ 	**<u>กรณี</u>** : ปัญหาที่พบผู้แจ้งสามารถแก้ไขเองได้ เจ้าหน้าที่จะให้คำแนะนำผ่านทางโทรศัพท์ กรณี : ปัญหาที่ผู้แจ้งไม่สามารถแก้ไขได้ จะนัดหมายวันเวลาที่สะดวกให้เจ้าหน้า	พนักงาน IT		

	ที่เข้าไปดำเนินการซ่อม			
	ศึกษาข้อมูลและปัญหาก่อนดำเนินการซ่อมเพื่อนลดระยะเวลาในการซ่อม ให้รวดเร็ว	พนักงาน IT	1-3 วัน	
		พนักงาน IT		
	เข้าระบบแจ้งซ่อมคอมพิวเตอร์	พนักงาน IT		

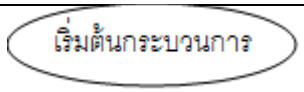
10.2. 2 งานซ่อมบำรุงประจำเดือน (iT Audit)

แผนผังลำดับงาน **(Flow Chart)**	**ขั้นตอน/ วิธีดำเนินงาน**	**ผู้รับผิดชอบ**	**ระยะเวลาดำเนินการ**	**เอกสารที่เกี่ยวข้อง**

				
	แผนการตรวจสอบระบบเทคโนโลยีสารสนเทศจัดทำแผนเข้าตรวจระบบสารสนเทศประจำปี	หน. IT	ก่อนเริ่มปีงปม.	
	เข้าตรวจสอบคอมพิวเตอร์ด้าน Hardware และ Software และระบบ Network เป็นต้น	พนักงาน IT	1วัน	
	สรุปผลการตรวจ_ด้าน Hardware และ Software และ Network ให้ผู้ใช้งานทราบ	พนักงาน IT		

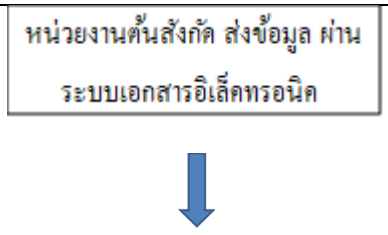
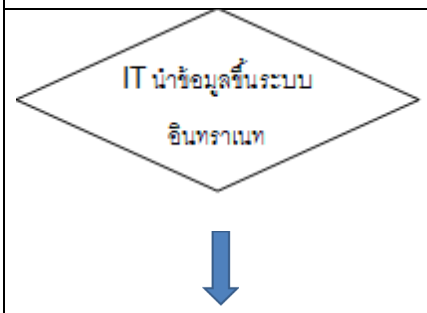
	กรณี ตรวบพบ Software ละเมิดลิขสิทธิ์ หรือ Software ที่ไม่มีความจำเป็นในการทำงาน Uninstall ออก	พนักงาน IT		
	ทำแบบฟอร์มประเมินความพึงพอใจในการปฏิบัติงาน	พนักงาน IT		
		พนักงาน IT		

10.2.3. การบริหารจัดการระบบข้อมูลอินทราเนทผ่านระบบเอกสารอิเล็คทรอนิคหรืออีเมลล์

แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
				

				
หน่วยงานต้นสังกัด ส่งข้อมูล ผ่านระบบเอกสารอิเล็คทรอนิค 	ส่งประกาศทาง E-mail หรือระบบการจัดการเอกสารอิเล็คทรอนิคส์ โดยแจ้งหัวข้อประกาศวันที่ที่ต้องการลงข้อมูล	พนักงานพัสดุ		
IT นำข้อมูลขึ้นระบบอินทราเนท 	IT ทำการอัปโหลดประกาศลงเว็ปไซด์ในระบบอินทราเนท	พนักงาน IT	1วัน	
ตรวจสอบประกาศหน้าเว็ปไซด์ 	ตรวจสอบความสมบูรณ์ของประกาศที่ทำการอัปโหลดลงเว็ปไซด์ในระบบอินทราเนท	พนักงาน IT	1วัน	
สิ้นสุดกระบวนการ				

10.2.4. การบริหารจัดการระบบข้อมูลทางอินเตอร์เนท

แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลา	เอกสารที่เกี่ยวข้อง
				
	ส่งประกาศทาง E-mail หรือระบบการจัดการเอกสารอิเล็คทรอนิคส์ โดยแจ้งหัวข้อประกาศวันที่ที่ต้องการลงข้อมูล	พนักงานทุกหน่วยงาน		
	IT ทำการอัปโหลดประกาศลงเว็ปไซต์ในระบบอินทราเนท	พนักงาน IT	1วัน	
	ตรวจสอบความสมบูรณ์ของประกาศที่ทำการอัปโหลดลงเว็ปไซต์ในระบบอินทราเนท	พนักงาน IT	1วัน	

สิ้นสุดกระบวนการ				

10.2.5. การเผยแพร่และสื่อสารภายในองค์กร

แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
เริ่มต้นกระบวนการ ↓				
หน่วยงานต้นสังกัด Update ข้อมูลในระบบ Workplace ↓	ส่งประกาศทาง E-mail หรือระบบการจัดการเอกสารอิเล็คทรอนิคส์ โดยแจ้งหัวข้อประกาศวันที่ที่ต้องการลงข้อมูล	พนักงานทุกหน่วยงาน		
IT สรุปข่าวสารและสาระสำคัญ ↓	IT สรุปข้อมูลข่าวสารสำคัญทำหัวข้อ “งานกิจกรรม” และ News Letter ประจำเดือน	พนักงาน IT	1วัน และ 1 เดือน	
ตรวจสอบ Workplace งานกิจกรรม และ News Letter ประจำเดือน ↓	ตรวจสอบความสมบูรณ์ของประกาศ “งานกิจกรรม” ที่ Workplace และ News Letter ประจำเดือน	พนักงาน IT	1วัน และ	

			1 เดือน	
สิ้นสุดกระบวนการ				

10.2.6 ห้อง server และ Datacenter

การจัดทำระบบไอทีให้ได้ตามมาตรฐาน ISO27001 หรือ ISMS นั้น จะต้องมีงบประมาณที่สูงพอสมควร เพื่อแลกมาซึ่งความมั่นคงปลอดภัยของสารสนเทศ เนื่องจาก บริษัทอู่กรุงเทพ จำกัด เป็นองค์กร ที่มีขนาดไม่ใหญ่มากนัก แต่อยากจะได้การรับรองมาตรฐาน และต้องการใช้งบประมาณให้คุ้มค่า ในการทำห้อง Server **และ Datacenter** อย่างถูกต้อง ซึ่งเป็นส่วนหนึ่งที่ Auditor จะต้องเข้ามาตรวจเป็นอันดับแรก 07’8;imeshv’.oi^xc[[fy’9jvwxouh

มุมมองจากด้านนอกห้อง

1) ห้อง Server ห้ามมีป้ายบอกว่าเป็นห้อง "Server Room" เพื่อป้องกันการแอบเข้ามาขโมยทรัพย์สิน หรือเข้ามาทำลายในกรณีเกิดเหตุการณ์ประท้วงของพนักงาน

2) ประตูห้องจะต้องถูกล็อคไว้ตลอดเวลา ควรจะใช้ Key Card, Key Pad หรือล๊อคด้วยกุญแจก็ได้

3) ห้อง Server ควรทำอย่างมิดชิด เมื่อมองจากด้านนอกเข้าไปข้างในจะต้องไม่ให้รู้ว่าเป็นห้อง Server หรือหากผนังเป็นกระจกใส ต้องทำการติดฟิล์มทึบทับไว้

4) ประตูทางเข้า จะต้องมีกล้องวงจรปิดบันทึกภาพบริเวณประตูเข้าออกห้อง

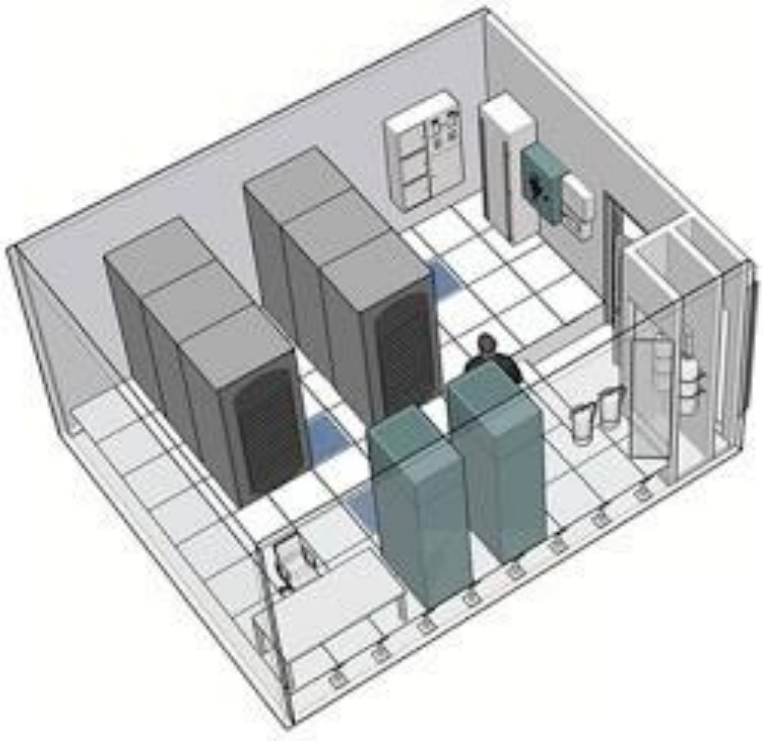
<u>ภายในห้อง</u>

1) ขนาดของห้อง ควรมีขนาดความกว้างและความสูง พอเหมาะสำหรับวางอุปกรณ์ต่างๆ และมีจุดสำหรับนั่งทำงานเป็นครั้งคราวได้ ห้องไม่ควรกว้างหรือแคบจนเกินไป

2) พื้นห้อง จะต้องยกสูงจากพื้นปกติ อย่างน้อย 15 ซม. ผู้ตรวจประเมินจะเปิดดูพื้นว่ามีสิ่งของใดๆ มาเก็บไว้ใต้พื้นหรือไม่ ถ้ามีสายสัญญาณต่างๆ ให้จัดเก็บให้เป็นระเบียบเรียบร้อย

3) ห้อง server ควรแยกออกจากห้องอื่นที่มีเพดานติดกัน หากห้องอยู่ติดกัน จะต้องมีการป้องกันผู้ไม่หวังดีเล็ดลอดเข้าทางเพดาน

4) สายไฟ สายสัญญาณต่างๆ จะต้องจัดเก็บให้เป้นระเบียบเรียบร้อย เก็บไว้ในราง หรือ มัดรวมกัน ถ้ามีการเดินสายไฟต่างๆ บนพื้น หรือผนัง จะต้องมี Cover ครอบไว้

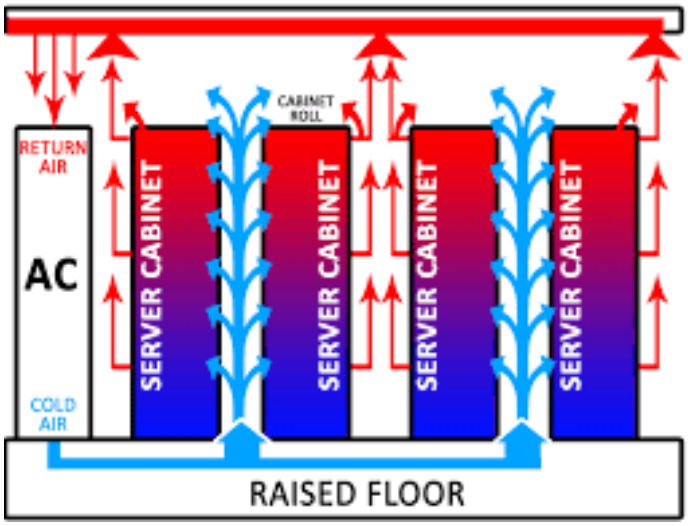


<u>เครื่องปรับอากาศ (Air condition)</u>

1) โดยปกติห้อง Server จะต้องมีการควบคุมอุณหภูมิภายในห้องอยู่ที่ 20 - 22 องศา

2) การปรับอากาศ ให้ทำการปล่อยความเย็นมาทางด้านล่างไปยังตู้ Rack เพื่อไล่ความร้อนขึ้นสู่ด้านบน

3) เครื่องปรับอากาศ ควรแยกจากระบบปรับอากาศอื่นๆ เพื่อควบคุมอุณหภูมิของห้อง Server โดยเฉพาะ



<u>กรณีที่ใช้แอร์แขวน หรือ แอร์ตั้ง</u>

4) จะต้องปรับมุมหรือหันตู้ Rack ให้ตรงช่องแอร์ที่ความเย็นส่งถึง ห้ามวางตู้ Rack ไว้ใต้แอร์ (กันน้ำแอร์หยดใส่ด้วย)

5) ถ้าไม่มีการติดตั้งระบบปรับอากาศที่สมบูรณ์ ควรติดตั้งแอร์ 2 ตัว ตั้งเวลาเปิดปิดสลับทำงาน กรณีแอร์ตัวใดตัวหนึ่งเสีย ก็ยังมีอีกตัวเป็นเครื่องสำรองได้

6) การควบคุมอุณหภูมิภายในห้อง ให้ติดตั้งเทอร์โมมิเตอร์ ที่สามารถวัดความชื้นได้ และแสดงค่าอุณหภูมิ min-max ได้ และจัดควรมีการจดบันทึกอุณหภูมิประจำวันไว้อ้างอิง ถ้าเทอโมมิเตอร์ที่ใช้แบตเตอรี่ ควรตรวจสอบแบตเตอรี่ด้วยว่าหมดหรือยัง และเครื่องเทอร์โมมิเตอร์ต้องผ่านการ Calibrate ก่อนนำมาใช้งาน

7) ควรมีแผนทำความสะอาดแอร์เดือนละครั้ง หรือ 3 เดือนครั้งแล้วแต่ อาจจะใช้บริการ MA กับบริษัทผู้รับเหมาก็ได้ และควรมีการบันทึกเก็บไว้เป็นหลักฐานทุกครั้งที่ทำความสะอาด

<u>การประเมินความเสี่ยง ให้ประเมินตามหัวข้อต่อไปนี้</u>

- กรณีแอร์เสีย ประเมินว่ามีผลอย่างไรกับระบบคอมพิวเตอร์ และมีวิธีการจัดการอุณหภูมิห้องอย่างไร
- กรณีมีแอร์ 1 ตัว จะต้องมีมาตรการในการดูแลรักษา ให้แอร์ทำงานปกติ (ให้ทำตามข้อ 6, 7)

<u>ตู้ Rack</u>

1) ปัจจุบัน ตู้ Rack ได้ผลิตออกมาเพื่อรองรับมาตรฐานนี้อยู่แล้ว แต่ที่แนะนำคือ ด้านหน้าจะต้องเป็นกระจกใสหรือมัว ขอบประตูมีช่องระบายอากาศเล็กๆ ประตูหลังทั้งบานจะมีรูระบายอากาศเช่นกัน

2) ตู้ Rack ทุกตู้ที่อยู่ในห้อง ประตูจะต้องถูกล็อคกุญแจไว้ กรณีที่ผู้ตรวจประเมินเดินเข้ามา เห็นเปิดค้างไว้ (แค่แง้มก็ไม่ได้)

3) ตู้ Rack จะต้องมีพัดลมดูดอากาศ ติดตั้งไว้ โดยทั่วไปจะมีพัดลมประมาณ 2 ตัวมาพร้อมกับตู้

<u>อุปกรณ์อื่นๆ ที่อยู่ในห้อง</u>

1) Wiring - สายไฟ สายสัญญาณ หรือสายแลน จะต้องมีการจัดเก็บให้เป็นระเบียบเรียบร้อย ใส่ในราง หรือ มี cover ครอบไว้

2) Asset - อุปกรณ์ทุกชิ้นในห้อง จะต้องมีการลงทะเบียนบัญชีทรัพย์สินทางด้านสารสนเทศ และติดป้ายไว้ในแต่ละอุปกรณ์

3) Fire protect - เครื่องดับเพลิงอัตโนมัติ เดิมที่ติดตั้งบนฝ้าเพดาน ต้องตรวจสอบดูว่าเป็นชนิดสารเคมีที่ไม่มีผลเสียหายแก่อุปกรณ์อิเลคทรอนิคส์ หรือใช้สารดับเพลิง class A, B, C แต่ถ้าไม่ได้ติดตั้งระบบออโต้ ก็ให้มีถังมาวางไว้หน้าห้อง หรือบริเวณที่สะดวกใช้งานได้

4) Power Supply - กรณีไม่มีเครื่องกำเนิดไฟฟ้า (เครื่องปั่นไฟ) ให้ใช้เครื่องสำรองไฟ (UPS) ที่มีกำลังสำรองไฟฟ้าตามความเหมาะสม เช่น สำรองไฟได้ 2 ชม. เป็นต้น และควรแยกออกจากตู้ Rack ที่มี Server หรือแยกไว้คนละตู้นั่นเอง

5) อุปกรณ์อื่น ของเล็กๆน้อยๆ ที่จำเป็น เช่น เอกสาร, เทป backup, แผ่น CD/DVD ฯลฯ ควรมีตู้จัดเก็บอย่างมิดชิด

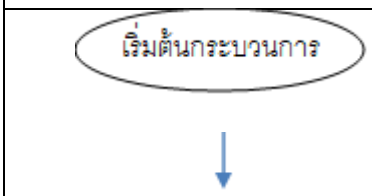
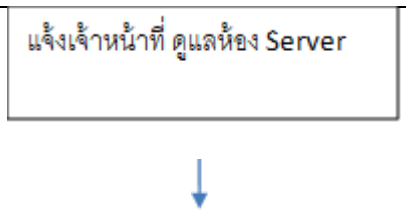
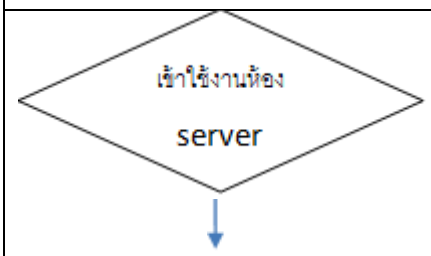
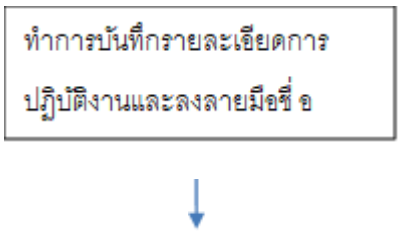
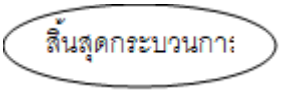
<u>เรื่องอื่นๆ ที่ผู้ดูแลต้องทำ</u>

1) มีสมุดบันทึกการเข้าออกห้อง Server ทุกครั้งลงในแบบฟอร์ม (วันหนึ่งจะเข้าออกกี่รอบก็ต้องจด) โดยระบุรายละเอียด ดังนี้

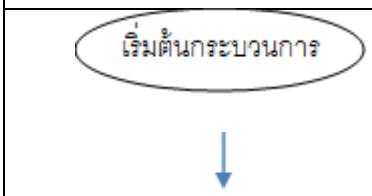
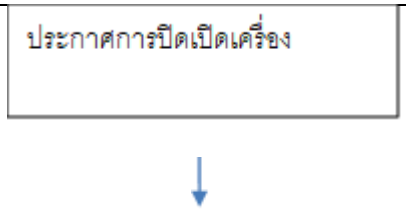
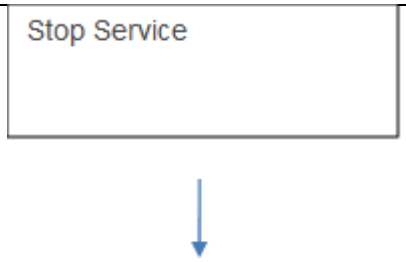
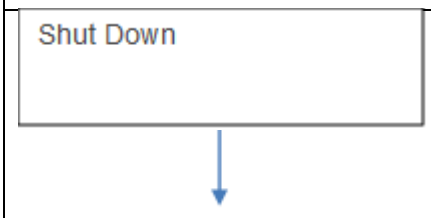
- ชื่อ-นามสกุล (ลงชื่อทุกคนที่เข้ามาในห้อง)
- เวลาเข้า – เวลาออก
- เหตุผลที่เข้ามาในห้อง

2) ระบบไฟฟ้าที่จ่ายไปยังห้อง Server จะต้องแยกอุปกรณ์ตัดไฟ (Breaker) ไว้ต่างหาก ห้ามรวมกับระบบไฟฟ้าอื่นๆ และผู้ดูแลและผู้เกี่ยวข้อง ต้องรับทราบด้วยว่า Breaker ติดตั้งไว้ที่ไหน

ขั้นตอนการขอเข้าใช้ห้อง Server

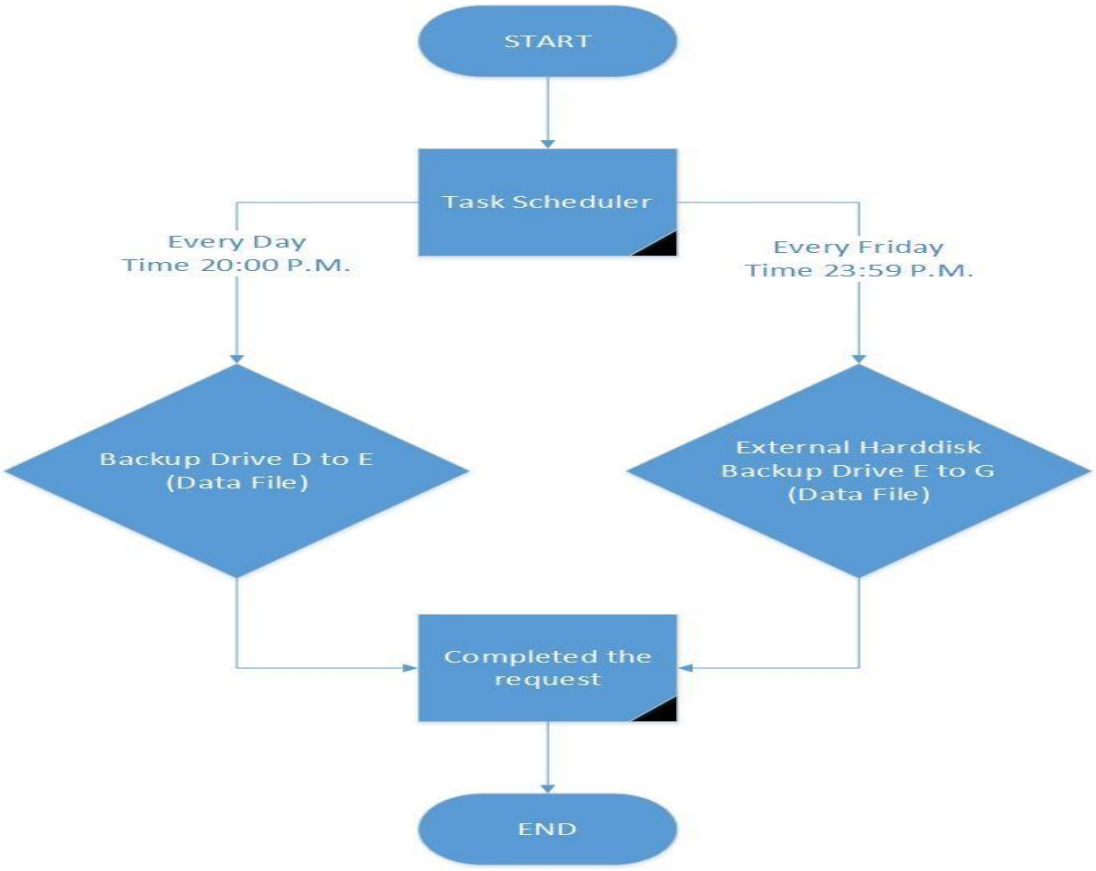
แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
				
	บุคลากรภายในแจ้งล่วงหน้าอย่างน้อย 1 ชั่วโมง บุคคลภายนอกแจ้งล่วงหน้า 1 วัน	พนักงาน IT		
				
	ทำการบันทึกรายละเอียดการปฏิบัติงานและลงลายมือชื่ อ หลังจากเข้าใชเสร็จแล้ว	พนักงาน IT		
				

ขั้นตอนการปิด - เปิดเครื่อง Server

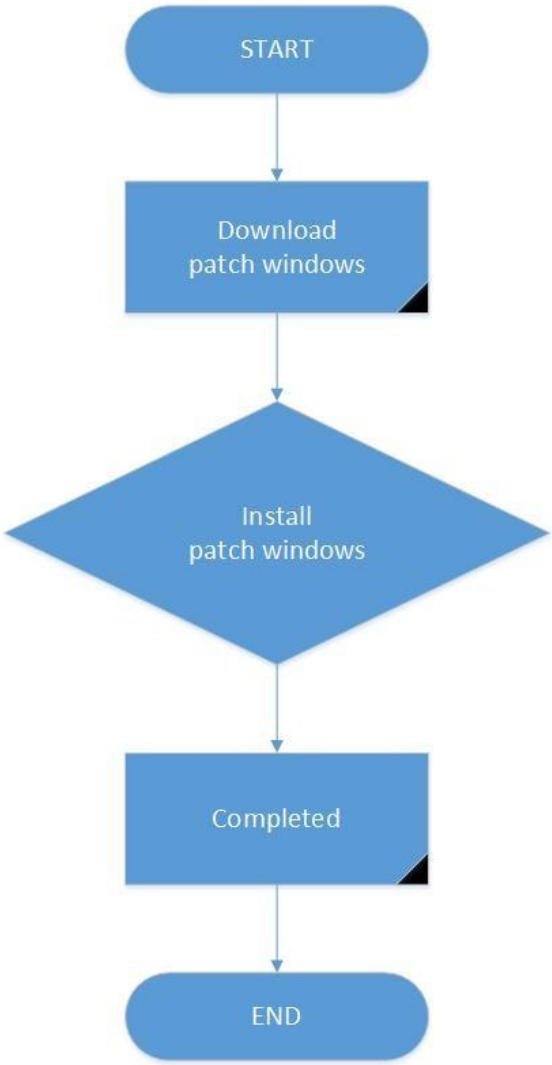
แผนผังลำดับงาน (Flow Chart)	ขั้นตอน/ วิธีดำเนินงาน	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ	เอกสารที่เกี่ยวข้อง
				
	แจ้งฝ่ายที่เกี่ยวข้อง ว่าจะปิดวันไหน เหตุผลใด ตั้งแต่เวลาใด ถึงเวลาใด	พนักงาน IT		
	ก่อนถึงวันทำการจริง ต้องเช็คแบคอัพ ว่าสมบูรณ์ไหม			
	Stop Service ต่างๆ เช่นพวก SQL และอื่นๆ	พนักงาน IT		
	ปิดเครื่อง	พนักงาน IT		

สิ้นสุดกระบวนการ				

10.2.7 ขั้นตอนการสำรองข้อมูล BDCSERVER01-03



10.2.8 ขั้นตอนการอัพเดท windows ทุกไตรมาส (ไตรมาสละ 1 ครั้ง)


START
Download
patch windows
Install
patch windows
Completed
END

10.2.9 ระบบวางแผนทรัพยากรองค์กร (ERP)

ระบบ ERP ที่ บ.อ.ท. นำมาใช้ประกอบด้วยระบบ MPR , HRM , CRM , SCM และ FRM ด้านบัญชีการเงิน ซึ่งมีวัตถุประสงค์ เพื่อช่วยในการบริหารงานอย่างมีประสิทธิภาพ

10.2.10 ระบบสารสนเทศเพื่อการบริหาร (MIS)

เป็นระบบจัดเก็บข้อมูลผลการดำเนินงานทั้ง 5 ด้าน ของ บ.อ.ท. ใช้ในการรายงานผลการดำเนินงานขององค์กรต่อฝ่ายบริหาร ทั้งในรูปแบบรายงานประจำเดือนและรายงานประจำปี รวมถึงรายงานเชิงเปรียบเทียบข้อมูลระหว่างเดือนเป็นรายปี ซึ่งแผนกติดตามและประเมินผล จะนำข้อมูลที่ได้ จากระบบ MIS มาจัดทำรายงานประเดือน และประจำปี เพื่อใช้ในการรายงานประชุมฝ่าย อย่างน้อยเดือนละ 1 ครั้ง

10.2.11 ระบบสารสนเทศสำหรับผู้บริหาร (EIS)

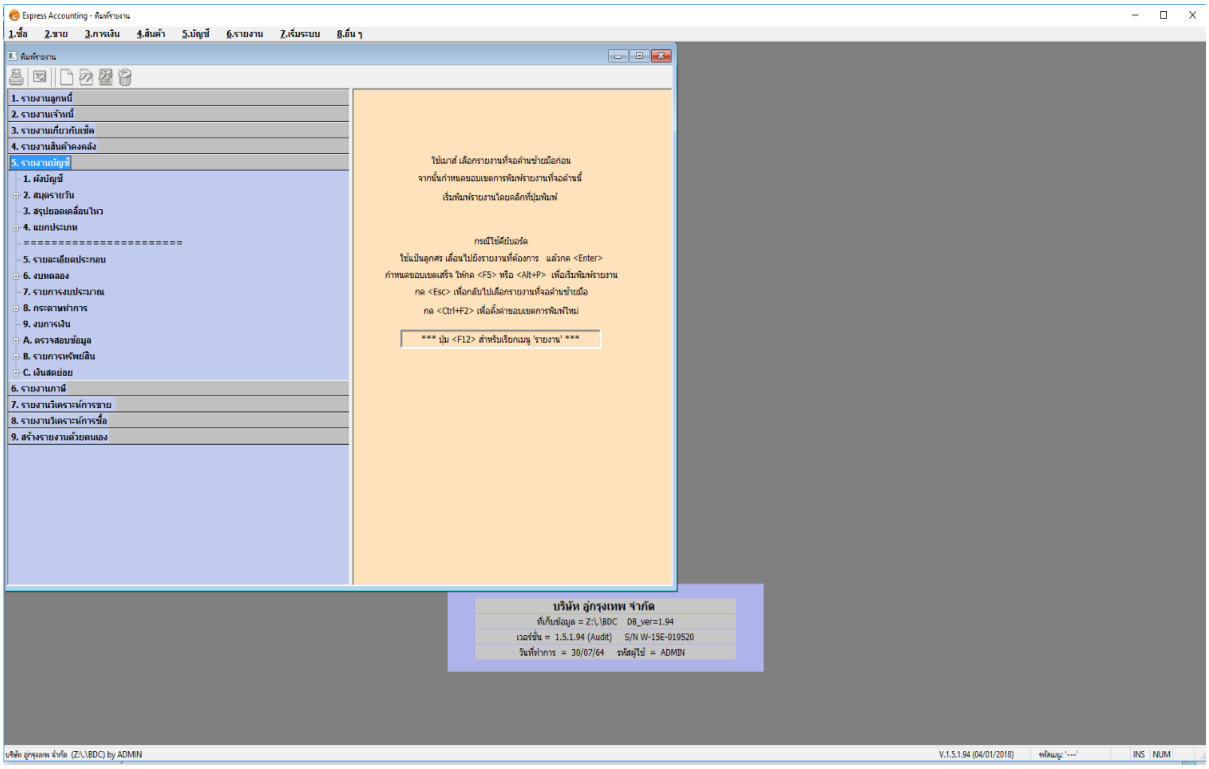
เป็นระบบสำหรับการประมวลผลข้อมูลที่จำเป็นโดยข้อมูลสำคัญนี้นำมาจาก 3 แหล่ง คือ
ข้อมูลจากการสำรวจความต้องการของผู้บริหาร ข้อมูลสำคัญขององค์กร และข้อมูลความต้องการใน อุตสาหกรรมเดียวกัน เพื่อประมวลผลใน 5 ด้าน และจัดทำให้อยู่ในรูปแบบที่ผู้บริหาร ของ บ.อ.ท. ต้องการ อาทิ การแสดงข้อมูลในรูปแบบกราฟ และรูปแบบการเปรียบเทียบ เป็นต้น เพื่อให้ ผู้บริหารองค์กรมีข้อมูลพร้อมใช้งานตลอดเวลา
โดยมีตัวอย่างหน้าจอของระบบฯ

10.2.12 ระบบบริหารจัดการทรัพยากรบุคคล (HRM)

ระบบ HRM เป็นระบบสนับสนุนการบริหารจัดการทรัพยากรบุคคล ประกอบด้วย ทะเบียนประวัติ โครงสร้างองค์กร การประเมินบุคลากรที่รองรับการปรับเกณฑ์การประเมินใหม่ ตลอดจน รายงานในด้านต่าง ๆ อาทิรายงานอัตรากำลัง รายงานการพัฒนาบุคคล รายงานสิทธิและสวัสดิการพนักงาน โดยมีตัวอย่างหน้าจอของระบบฯ

10.2.13 ระบบงานบัญชีและการเงิน (Express)

ระบบ Express เป็นระบบสนับสนุนการทำบัญชี ประกอบด้วย การลงบัญชีรายรับ รายจ่าย เจ้าหนี้ ลูกหนี้และบัญชีทรัพย์สิน เพื่อจัดทำงบการเงินรายงานผู้บริหารและสรุปงบการเงินประจำปี

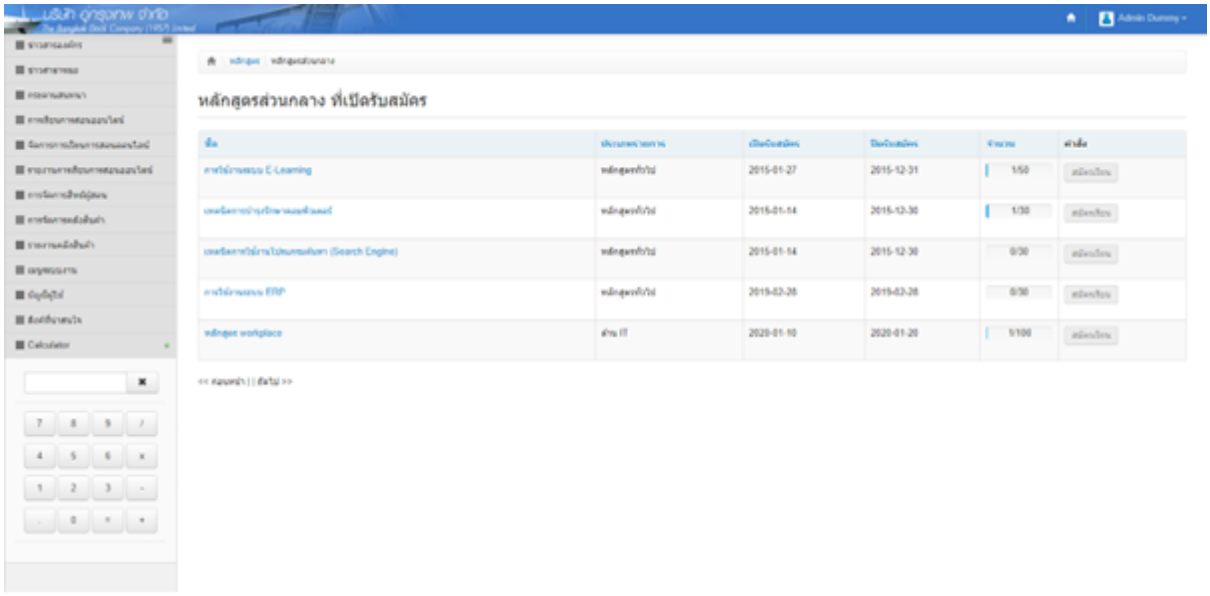


10.2.14 ระบบบริหารจัดการองค์ความรู้ (Knowledge Management)

เป็นระบบสนับสนุนการจัดทำองค์ความรู้ในรูปแบบไฟล์อิเลคทรอนิกส์ ซึ่งสามารถ นำไปเผยแพร่ให้หน่วยงานภายใน บ.อ.ท. เป็นการจัดเก็บองค์ความรู้ของบุคลากรผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์ในรูปแบบเอกสาร ทั้งนี้ แผนพัฒนาดิจิทัลฯ (สำหรับปี 2563) และแผนปฏิบัติการดิจิทัลฯ (สำหรับปี 2563) ได้กำหนดให้มีการปรับปรุงพัฒนาระบบบริหารจัดการองค์ความรู้ให้ครอบคลุมแนวทางการจัดทำและเผยแพร่องค์ความรู้ในรูปแบบอื่น ๆ

10.2.15 ระบบ e-Learning

เป็นระบบการเรียนการสอนแบบ On-Line โดยจัดทำเนื้อหาบทเรียนในลักษณะสื่อ On-Line ประกอบด้วยสื่อวิดีโอบทเรียน และแบบทดสอบก่อนและหลังการเรียนแบบ On-Line เพื่อให้พนักงานองค์กรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องสามารถเข้ามาศึกษาข้อมูลด้วยตนเองได้ตลอดเวลา โดยมีตัวอย่างหน้าจอของระบบฯ



10.2.16 ระบบบริหารจัดการความเสี่ยงองค์กร (Risk)

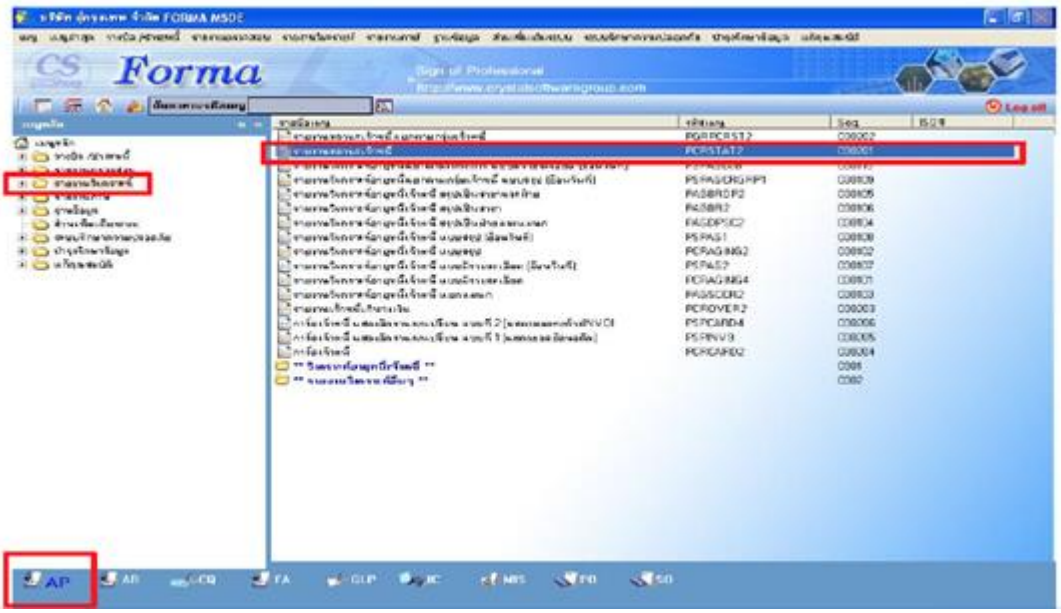
เป็นระบบสารสนเทศซึ่งรองรับการนำเข้าข้อมูลประเด็นความเสี่ยง โอกาสของการเกิด ความเสี่ยง (Likelihood) และผลกระทบจากความเสี่ยง (Impact) ตลอดจนการรายงานความก้าวหน้าในการดำเนินการกิจกรรมควบคุมและมาตรการในการบริหารและจัดการความเสี่ยง เพื่อให้หน่วยงานส่วนกลาง และผู้บริหารสามารถติดตามความก้าวหน้าของการดำเนินงานของทุกกิจกรรมควบคุม/มาตรการในระบบ และนำเสนอต่อที่ประชุมผู้บริหาร บ.อ.ท. คณะอนุกรรมการบริหารความเสี่ยง บ.อ.ท. และคณะกรรมการ บ.อ.ท. เห็นชอบตามลำดับ

10.2.17 ระบบควบคุมและตรวจสอบภายใน (Audit)

ระบบควบคุมภายใน เป็นระบบที่สามารถควบคุมและตรวจสอบการทำงานได้ในระดับหน่วยงานเพื่อให้เกิดประสิทธิภาพและประสิทธิผลในการปฏิบัติงาน โดยมีหน่วยงานหลักที่รับผิดชอบ ได้แก่ แผนกบริหารความเสี่ยงและควบคุมภายในและมีวัตถุประสงค์เพื่อประเมินความเพียงพอและประสิทธิผลของระบบงานและกิจกรรมต่างๆ ของ บ.อ.ท. โดยให้แต่ละส่วนงานที่เกี่ยวข้องนำเข้าข้อมูล ที่มีผลกระทบต่อส่วนงานนั้นๆ เพื่อทำการควบคุมเป็นรายไตรมาส และกรอกวิธีการควบคุม ตลอดจนประเมินผลการควบคุมว่าเพียงพอหรือไม่ มีปัญหาในการดำเนินการอย่างไร หากไม่สามารถควบคุมได้ หรือ ปัญหานั้นๆ

มีผลกระทบต่อองค์กร จะมีขั้นตอนในการพิจารณาเพื่อนำเข้าที่ประชุมเพื่อตั้งเป็นความเสี่ยงองค์กรต่อไป

1.1.1. เลือกเมนู AP -> รายงานวิเคราะห์ -> รายงานสถานะเจ้าหนี้



10.2.18 ระบบ e-Saraban

ระบบสารสนเทศสำหรับการบริหารจัดการงานด้านเอกสาร เพื่อรับ-ส่งเอกสาร ภายในองค์กรโดยอยู่ในรูปแบบอิเล็กทรอนิกส์ เพื่อให้สามารถติดตามสถานะของหนังสือและสามารถลด ระยะเวลาในการปฏิบัติงานได้ โดยมีตัวอย่างหน้าจอของระบบฯ ดังแสดงในภาพที่ 3.4-11

10.2.19 ระบบ e-Document

e-Document หมายถึง เอกสารในรูปแบบของเอกสารอิเล็กทรอนิกส์ อาทิ ไฟล์ เอกสาร ไฟล์รูปภาพ ฯลฯ ซึ่งมีการใช้งานอย่างแพร่หลาย โดยปกติเอกสารต่าง ๆ จะมีการเก็บรักษาไว้ในตู้ หรือชั้นเอกสารขององค์กร ซึ่งจัดเรียงไว้เป็นหมวดหมู่เพื่อให้ค้นหาได้ง่ายและสะดวกในการนำไปใช้ การอยู่ในรูปแบบกระดาษทำให้จะต้องเตรียมที่เก็บเอกสารเหล่านี้ และเมื่อเอกสารเหล่านี้เพิ่มมากขึ้นตามกาลเวลา ทำให้เก็บรักษาลำบาก นอกจากนี้ยังต้องมีระยะเวลาเก็บรักษาและทำลายให้เป็นไปตามนโยบายและกฎระเบียบขององค์กรนั้น ๆ ด้วย ซึ่งจะเห็นได้ว่า การเก็บเอกสารที่เป็นกระดาษนั้นทำให้สิ้นเปลืองกระดาษและพื้นที่ในการเก็บรักษาเป็นจำนวนมาก การจะนำไปใช้ก็ค้นหาค่อนข้างลำบาก เนื่องจากบางชิ้นอาจเก็บไว้นานจนลืมไปแล้วว่าอยู่ที่ไหน ทั้งยังต้องเสียเวลาในการค้นหา ด้วยเหตุนี้ จึงได้มีการพัฒนาเทคโนโลยี e- Document ขึ้นมาช่วยในการจัดเก็บเอกสาร เพื่อให้สามารถบริหารจัดการระบบเอกสารให้สามารถสืบค้น

ได้อย่างง่ายดายและรวดเร็วยิ่งขึ้น ซึ่งจะช่วยเพิ่มประสิทธิภาพกระบวนการทำงานให้ดีขึ้นอีกด้วย โดยมีตัวอย่างหน้าจอของระบบฯ ดังแสดงในภาพที่ 3.4-12

10.2.20 ระบบ E-mail

ปัจจุบัน บ.อ.ท. ใช้บริการระบบ E-mail บนระบบ Cloud SaaS (Microsoft Exchange) โดยใช้ชื่อ Domain Name ของ E-mail เป็นชื่อเดียวกันกับ Website หลักของหน่วยงาน

10.2.21 ระบบ Web Site

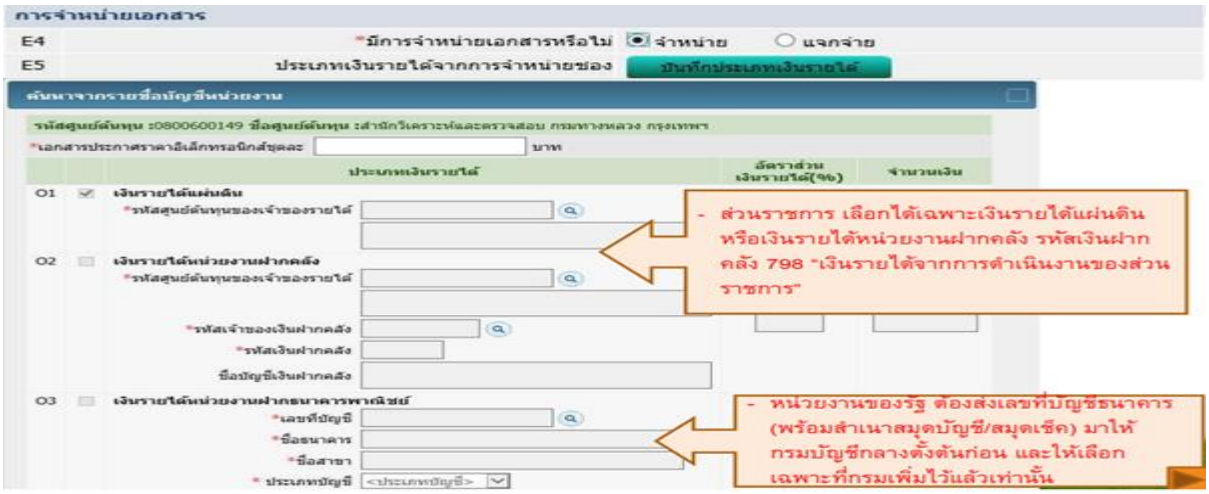
เป็นระบบสารสนเทศสำหรับการประชาสัมพันธ์ข้อมูลข่าวสารให้บุคคลภายในและ ภายนอก โดยแบ่งเป็น 5 หมวดหมู่ คือ เกี่ยวกับ บ.อ.ท. / ข่าวและกิจกรรม / ผลิตภัณฑ์และบริการ / สาระ น่ารู้ / คำถาม / และติดต่อ บ.อ.ท. เพื่อให้ประชาชนทั่วไปที่สนใจได้รับรู้ข้อมูลข่าวสารของ บ.อ.ท. โดย มีตัวอย่างหน้าจอของระบบฯ

ทั้งนี้ แผนพัฒนาดิจิทัลฯ (สำหรับปี 2563) และแผนปฏิบัติการดิจิทัลฯ (สำหรับปี 2563) ได้กำหนดให้มีการพัฒนาระบบบริหารจัดการองค์ความรู้และระบบ e-Learning เพื่อรองรับการมุ่งสู่ องค์กรแห่งการเรียนรู้ (Learning Organization) และบูรณาการระบบบริหารจัดการความเสี่ยงและระบบควบคุมและตรวจสอบภายในเข้ากับระบบงานอื่น ๆ เพื่อการนำเข้าข้อมูลสารสนเทศได้แบบทันท่วงทีและเป็น อัตโนมัติ

10.2.22 ระบบงาน e-GP

เป็นระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ซึ่งจัดทำขึ้นเพื่อให้หน่วยงานภาครัฐและเอกชนสามารถเข้าถึงแหล่งข้อมูลการจัดซื้อจัดจ้าง และพัสดุภาครัฐได้อย่างรวดเร็ว ถูกต้อง ครบถ้วน เป็นศูนย์ข้อมูลการจัดซื้อจัดจ้างภาครัฐที่มีระบบบริหารจัดการรหัสสินค้าและบริการภาครัฐ เก็บข้อมูลของหน่วยจัดซื้อและข้อมูลผู้ค้าสำหรับการจัดซื้อจัดจ้างรูปแบบต่าง ๆ เชื่อมต่อข้อมูลกับแหล่งข้อมูลภายนอกที่เกี่ยวข้อง โดยมีเป้าหมายเพื่อเพิ่มความโปร่งใส ลดปัญหาทุจริตคอร์รัปชั่น ลดความผิดพลาดใน

การปฏิบัติตามระเบียบ และลดความซ้ำซ้อนการบันทึก

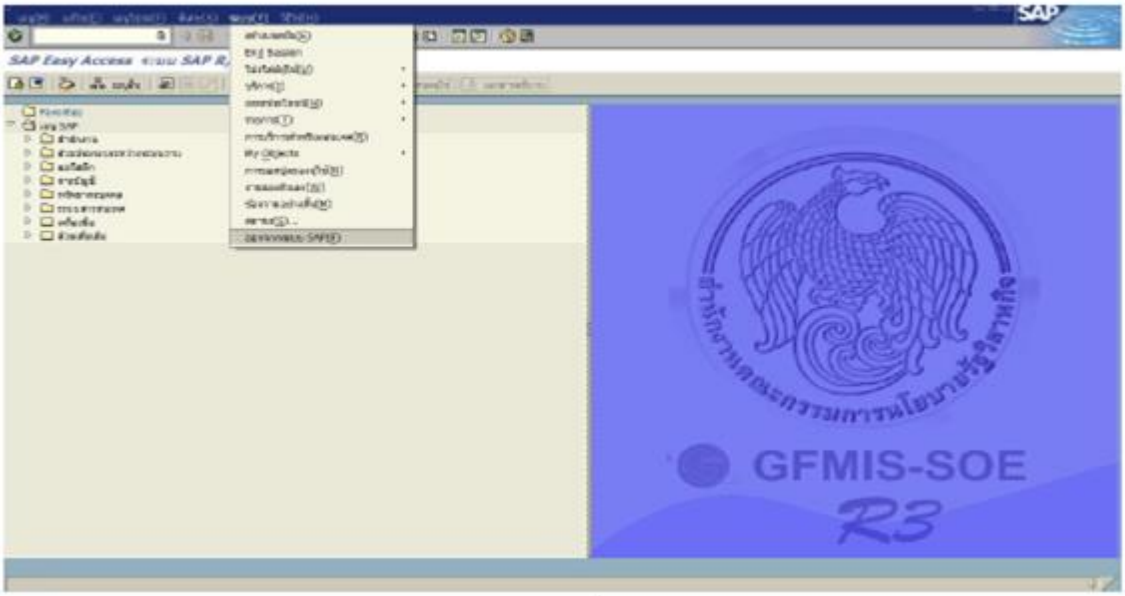


10.2.23 ระบบงาน GFMIS

ระบบสารสนเทศเพื่อรองรับการบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ และปรับปรุงระบบการจัดการด้านการเงินการคลังของภาครัฐให้มีความทันสมัยและมีประสิทธิภาพยิ่งขึ้น และครอบคลุมกระบวนการดำเนินงานและการจัดการภาครัฐด้านการงบประมาณ การบัญชี การจัดซื้อจัด จ้าง การเบิกจ่าย และการบริหารทรัพยากร ให้เป็นไปในทิศทางเดียวกับนโยบายปฏิรูปราชการที่เน้น ประสิทธิภาพและความคล่องตัวในการดำเนินงาน รวมทั้งมุ่งหวังให้เกิดการใช้ทรัพยากรภายในองค์กรอย่างคุ้มค่าเพื่อให้ได้มาซึ่งข้อมูลสถานภาพการคลังภาครัฐที่ถูกต้องรวดเร็ว สามารถตอบสนองนโยบายการบริหารเศรษฐกิจของประเทศ

10.2. ระบบงาน GFMIS-SOE

เป็นระบบ GFMIS เพื่อรองรับข้อมูลรัฐวิสาหกิจ (GFMIS–SOE) ของสำนักงาน คณะกรรมการนโยบายรัฐวิสาหกิจ เพื่อการกำกับดูแลของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ที่จะ ควบคุมติดตาม ดูแล ประเมินผล ประสิทธิภาพ ประสิทธิผล การใช้จ่ายงบประมาณ การเงิน การนำส่งรายได้ ผลประกอบการของรัฐวิสาหกิจในแต่ละช่วงเวลา รวมถึงการรวบรวมข้อมูลเพื่อจัดทำข้อมูลบริหารรวมด้าน การเงิน การคลัง การงบประมาณ จากหน่วยงานรัฐวิสาหกิจทั่วประเทศ


SAP Easy Access
GFMIS-SOE
R3