NECTEC
a member of NSTDA

มาตรฐานการรักษาความมั่งคงปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5)
ประจำปี 2550

จัดพิมพ์และเผยแพร่โดย

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะอนุกรรมการด้านความมั่งคง ใน คณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์

NECTEC
a member of NSTDA

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี
112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน
ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 02-564-6900
โทรสาร 02-564-6901..2

National Electronics and Computer Technology Center
National Science and Technology Development Agency
Ministry of Science and Technology
112 Thailand Science Park, Phahon Yothin Road,
Klong Luang, Pathumthani 12120, THAILAND.
Tel. +66-2-564-6900
Fax. +66-2-564-6901..2

ISBN 978-974-229-584-4
9 789742 295844
เอกสารเผยแพร่

ThaiCERT
http://www.thaicert.nectec.or.th
e-mail: thaicert@nectec.or.th

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550

จัดพิมพ์และเผยแพร่โดย

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ
ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะอนุกรรมการด้านความมั่นคง
ใน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550

พิมพ์เผยแพร่โดย
หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ISBN: 978-974-229-584-4

พิมพ์ครั้งที่ 1 (ธันวาคม 2550)
จำนวน 1,000 เล่ม
เอกสารเผยแพร่

สงวนลิขสิทธิ์ พ.ศ. 2550 ตาม พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
ไม่อนุญาตให้คัดลอก ทำซ้ำ และดัดแปลง ส่วนใดส่วนหนึ่งของหนังสือฉบับนี้
นอกจากจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของลิขสิทธิ์เท่านั้น

Copyright©2007 by:
National Electronics and Computer Technology Center
National Science and Technology Development Agency
Ministry of Science and Technology
112 Thailand Science Park, Phahon Yothin Road, Klong 1, Klong Luang,
Pathumthani 12120, THAILAND.
Tel. +66(2)-564-6900 Fax. +66(2)-564-6901..2

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550/ หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.--กรุงเทพฯ : หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2550
64 หน้า
ISBN: 978-974-229-584-4
1. ความปลอดภัยในระบบคอมพิวเตอร์. 2. ระบบความปลอดภัย. I. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ
658.478 QA 76.9

จัดทำโดย

หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี
112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี 12120
โทรศัพท์ 02-564-6900 โทรสาร 02-564-6901..2
URL: http://thaicert.nectec.or.th/ e-mail: thaicert@nectec.or.th

คำนำ

สืบเนื่องจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้มีอำนาจหน้าที่ในการส่งเสริมและพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ และเสนอแนะมาตรการในการแก้ไขปัญหาและอุปสรรคใดๆ ต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งเสนอแนะการตรากฎหมายตลอดจนการกำกับดูแลธุรกิจบริการเกี่ยวกับการทำธุรกรรมทางออนไลน์ที่มีความเสี่ยงหรือเพื่อช่วยสร้างความเชื่อมั่นในการทำธุรกรรมดังกล่าวให้กับประชาชน และโดยที่ปัญหาและอุปสรรคสำคัญในการทำธุรกรรมทางอิเล็กทรอนิกส์ในปัจจุบัน คือ ปัญหาด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบเครือข่าย จึงเป็นเหตุให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้กำหนดนโยบายสำคัญในการพัฒนาและจัดทำมาตรฐานด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบเครือข่าย ทั้งนี้ เพื่อลดปัญหาอันเกิดจากภัยคุกคามหรือความเสี่ยงของระบบดังกล่าวลงให้มากที่สุด

ในการนี้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้มอบหมายให้คณะอนุกรรมการด้านความมั่นคงปลอดภัยทำการพัฒนามาตรฐานด้านความมั่นคงปลอดภัยดังกล่าวขึ้น โดยหน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ในฐานะฝ่ายเลขานุการของคณะอนุกรรมการชุดดังกล่าว เป็นหน่วยงานซึ่งทำการศึกษา วิจัย และพัฒนามาตรฐานดังกล่าวโดยอ้างอิงกับมาตรฐาน ISO/IEC 27001:2005 และ ISO/IEC 17799:2005 ทั้งนี้ เพื่อให้มาตรฐานความมั่นคงปลอดภัยที่พัฒนาขึ้นนั้นสอดคล้องกับมาตรฐานสากล

หลังจากคณะอนุกรรมการด้านความมั่นคงปลอดภัยได้พิจารณาปรับปรุงแก้ไขร่างมาตรฐานที่จัดทำขึ้นแล้ว ก็ได้นำร่างมาตรฐานดังกล่าวประชาสัมพันธ์และรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและประชาชนอีกจำนวนหลายครั้งด้วยกันและได้มีการเผยแพร่ร่างมาตรฐานดังกล่าวไปกว่า 4,000 ฉบับ โดยได้มีการปรับปรุงร่างมาตรฐานดังกล่าวจำนวนหลายครั้งจนมีความสมบูรณ์และทันสมัย

จากนั้นคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ก็ได้พิจารณาให้ความเห็นชอบร่างมาตรฐานดังกล่าว เพื่อให้มีการดำเนินการตามขั้นตอนเพื่อประกาศให้ร่างมาตรฐานด้านความมั่นคงปลอดภัยที่จัดทำขึ้นนั้นเป็นมาตรฐานของประเทศไทยต่อไป

(นายพันธ์ศักดิ์ ศิริรัชตพงษ์)
ผู้อำนวยการ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
กรรมการและเลขานุการ
คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สารบัญ

กระบวนการจัดทำระบบบริหารจัดการความมั่งคงปลอดภัยสำหรับสารสนเทศ 9

ข้อ 1 ระบบบริหารจัดการความมั่งคงปลอดภัย 10

ข้อ 2 หน้าที่ความรับผิดชอบของผู้บริหาร 18

ข้อ 3 การตรวจสอบภายในระบบบริหารจัดการความมั่งคงปลอดภัย 20

ข้อ 4 การทบทวนระบบบริหารจัดการความมั่งคงปลอดภัยโดยผู้บริหาร 21

ข้อ 5 การปรับปรุงระบบบริหารจัดการความมั่งคงปลอดภัย 23

มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ 25

1. นโยบายความมั่นคงปลอดภัย (Security policy) 26

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy) 26

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) 26

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) 26

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties) 28

3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management) 29

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) 29

3.2 การจัดหมวดหมู่สารสนเทศ (Information classification) 30

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security).... 30
4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment).... 30
4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) 31
4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment) 32
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) 33
5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)..... 33
5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)..... 34
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management) 35
6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities) 35
6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)..... 36
6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance) 37
6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)..... 38
6.5 การสำรองข้อมูล (Back-up) 38
6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)..... 38
6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling) 39
6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)..... 40
6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)..... 41
6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring) 41

7. การควบคุมการเข้าถึง (Access control) 42
7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) 42
7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management) 43
7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) 43
7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control) 44
7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) 45
7.6 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and information access control) 46
7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking) 46
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) 47
8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems) 47
8.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (Correct processing in applications) 47
8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) 48
8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files) 48
8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes) 49
8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management) 50
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) 51

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses) 51
9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements) 51
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management) 52
10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management) 52
11. การปฏิบัติตามข้อกำหนด (Compliance) 53
11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements) 53
11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance) 55
11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations) 55
ภาคผนวก ก 57
ภาคผนวก ข 61

ส่วนที่ 1

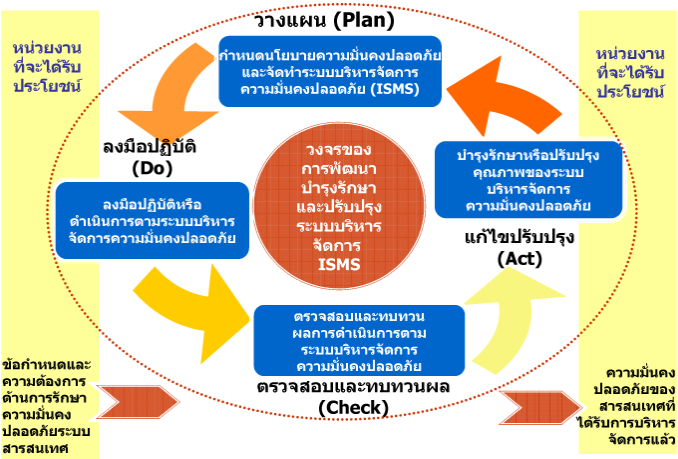
กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัย สำหรับสารสนเทศ (อ้างอิง ข้อกำหนดตามมาตรฐาน ISO/IEC 27001)

กระบวนการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

ข้อ 1 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1.1 ข้อกำหนดทั่วไป

องค์กรจะต้องกำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุง รักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ได้กำหนดไว้เป็นลายลักษณ์อักษร ภายในกรอบกิจกรรมการดำเนินการทางธุรกิจต่าง ๆ รวมทั้งความเสี่ยงที่เกี่ยวข้อง แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ตามแสดงใน รูปภาพที่ 1



รูปภาพที่ 1 แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act

1.2 กำหนดและบริหารจัดการ ระบบบริหารจัดการความมั่นคงปลอดภัย

1.2.1 กำหนดระบบบริหารจัดการความมั่นคงปลอดภัย (Plan)

องค์กรจะต้องปฏิบัติดังนี้

a) กำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี รวมทั้งอาจพิจารณาถึงสิ่งที่ไม่รวมอยู่ในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย

b) กำหนดนโยบายความมั่นคงปลอดภัย โดยพิจารณาถึงลักษณะของธุรกิจ องค์กร สถานที่ตั้ง ทรัพย์สิน และเทคโนโลยี นโยบายความมั่นคงปลอดภัยจะต้องมีองค์ประกอบดังนี้

   b.1 กรอบในการดำเนินการ ทิศทางและหลักการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ

   b.2 ข้อกำหนดทางธุรกิจ ข้อกำหนดในสัญญาต่างๆ ระเบียบปฏิบัติ ข้อบังคับ รวมทั้งกฎหมายของประเทศ

   b.3 การบริหารจัดการความเสี่ยงเชิงกลยุทธ์ในระดับองค์กร

   b.4 เกณฑ์ในการประเมินความเสี่ยง (ดูข้อ 1.2.1 c)

   b.5 การได้รับการอนุมัติจากผู้บริหาร

c) กำหนดวิธีการประเมินความเสี่ยงที่เป็นรูปธรรมขององค์กร

   c.1 ระบุวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการทางด้านความมั่นคงปลอดภัยขององค์กร

   c.2 กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระบุระดับความเสี่ยงที่ยอมรับได้

d) ระบบความเสี่ยง

   d.1 ระบุทรัพย์สินที่อยู่ในขอบเขตของระบบบริหารจัดการความปลอดภัยรวมทั้งผู้เป็นเจ้าของทรัพย์สินเหล่านั้น

   d.2 ระบุภัยคุกคามที่มีต่อทรัพย์สินเหล่านั้น

   d.3 ระบุจุดอ่อนที่ภัยคุกคามอาจจะใช้ให้เป็นประโยชน์

   d.4 ระบุผลกระทบที่ก่อให้เกิดความสูญเสียทางด้านความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

e) วิเคราะห์และประเมินความเสี่ยง

   e.1 ประเมินผลกระทบที่มีต่อธุรกิจซึ่งอาจเป็นผลจากความล้มเหลว

ในการรักษาความมั่นคงปลอดภัย โดยพิจารณาผลของการสูญเสียความลับ ความสมบูรณ์ ความพร้อมใช้ของทรัพย์สินเหล่านั้น

e.2 กำหนดความน่าจะเป็นของความเสี่ยงอันเกิดจากความล้มเหลวในการรักษาความมั่นคงปลอดภัย

e.3 กำหนดระดับความเสี่ยง

e.4 กำหนดว่าความเสี่ยงเหล่านั้น สามารถยอมรับได้หรือไม่ โดยใช้เกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้ในข้อ 1.2.1) c.2)

f) ระบุและประเมินทางเลือกในการจัดการกับความเสี่ยงการดำเนินการที่เป็นไปได้ อาจรวมถึง

f.1 ใช้มาตรการที่เหมาะสม

f.2 ยอมรับความเสี่ยงเหล่านั้น โดยมีเงื่อนไขว่า ความเสี่ยงเหล่านั้นจะต้องอยู่ภายในเกณฑ์ในการยอมรับความเสี่ยงที่กำหนดไว้ในข้อ 1.2.1) c.2)

f.3 หลีกเลี่ยงความเสี่ยงเหล่านั้น

f.4 โอนย้ายความเสี่ยงเหล่านั้นไปสู่ผู้อื่น เช่น บริษัทประกันภัย เป็นต้น

g) เลือกวัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยเพื่อจัดการกับความเสี่ยง วัตถุประสงค์และมาตรการดังกล่าวสามารถเลือกมาจากมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ในตอนท้ายของมาตรฐานฉบับนี้

h) ขอการอนุมัติและความเห็นชอบสำหรับความเสี่ยงที่ยังหลงเหลืออยู่ในระบบบริหารจัดการความมั่นคงปลอดภัย

i) ขอการอนุมัติเพื่อลงมือปฏิบัติและดำเนินการ

j) จัดทำเอกสาร SoA (Statement of Applicability) แสดงการใช้งานมาตรการตามที่แสดงไว้ในส่วนของมาตรฐานการรักษาความมั่นคง

ปลอดภัยในการประกอบธุรกรรมทางด้านอิเล็กทรอนิกส์ เอกสารดังกล่าวควรมีองค์ประกอบดังนี้

j.1 วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยตามที่ได้เลือกไว้ในข้อ 1.2.1) g) รวมทั้งเหตุผลการใช้งาน

j.2 วัตถุประสงค์และมาตรการทางด้านความมั่นคงปลอดภัยที่ได้ใช้งานอยู่ในปัจจุบัน

j.3 วัตถุประสงค์และมาตรการความมั่นคงปลอดภัยที่ไม่มีการใช้งานรวมทั้งเหตุผลที่ไม่มีการใช้งาน

1.2.2 ลงมือปฏิบัติและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัย องค์กรควรปฏิบัติดังนี้ (Do)

a) จัดทำแผนการจัดการความเสี่ยงซึ่งกล่าวถึงการดำเนินการเชิงบริหารจัดการ ทรัพยากรที่จำเป็น หน้าที่ความรับผิดชอบ และลำดับการดำเนินการเพื่อบริหารจัดการความเสี่ยงที่พบ

b) ลงมือปฏิบัติตามแผนการจัดการความเสี่ยงเพื่อบรรลุในวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

c) ลงมือปฏิบัติตามมาตรการที่เลือกไว้ในข้อ 1.1.2) g) เพื่อบรรลุวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยของมาตรการดังกล่าว

d) กำหนดวิธีการในการวัดความสัมฤทธิผลของมาตรการที่เลือกมาใช้งาน การวัดดังกล่าวจะต้องสามารถสร้างผลลัพธ์ที่สามารถเปรียบเทียบได้ รวมทั้งสามารถสร้างผลลัพธ์เดิมขึ้นมาอีกครั้งหนึ่งได้

e) จัดทำและลงมือปฏิบัติตามแผนการอบรมและสร้างความตระหนัก (ดูข้อ 2.2.2)

f) บริหารการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย

g) บริหารทรัพยากรสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย (ดูข้อ 2.2)

h) จัดทำและลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ ซึ่งช่วยในการตรวจจับและรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย (ดูข้อ 1.2.3 a)

1.2.3 เฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยองค์กรควรปฏิบัติดังนี้ (Check)

a) ลงมือปฏิบัติตามขั้นตอนปฏิบัติและมาตรการอื่นๆ สำหรับการเฝ้าระวังและทบทวน เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสามารถ

a.1 ตรวจจับข้อผิดพลาดจากการประมวลผล

a.2 ระบุการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

a.3 ช่วยให้ผู้บริหารสามารถระบุได้ว่ากิจกรรมทางด้านความมั่นคงปลอดภัยที่มอบหมายให้กับบุคลากรขององค์กรเป็นไปตามที่คาดหมายไว้หรือไม่

a.4 ตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยโดยอาศัยตัวบ่งชี้ต่างๆ เพื่อช่วยในการตรวจจับเหตุการณ์ต่างๆ ที่ไม่คาดคิด

a.5 ตรวจสอบได้ว่าการดำเนินการเพื่อแก้ไขการละเมิดทางด้านความมั่นคงปลอดภัยมีความสัมฤทธิผลหรือไม่

b) ดำเนินการทบทวนความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยนำสิ่งต่างๆ ต่อไปนี้มาพิจารณาร่วมด้วย ได้แก่ ผลการตรวจสอบก่อนหน้านี้ เหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดขึ้น ผลการวัดความสัมฤทธิผล คำแนะนำและผลตอบกลับจากองค์กรหรือหน่วยงานที่เกี่ยวข้อง เป็นต้น

c) วัดความสัมฤทธิผลของมาตรการทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบว่าเป็นไปตามข้อกำหนดทางด้านความมั่นคงปลอดภัย

d) ทบทวนผลการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนดไว้กับระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ โดยพิจารณาการเปลี่ยนแปลงของสิ่งต่อไปนี้ประกอบด้วย

d.1 องค์กร

d.2 เทคโนโลยี

d.3 วัตถุประสงค์และกระบวนการทางธุรกิจ

d.4 ภัยคุกคามที่ระบุไว้ก่อนหน้านี้ กับสภาพการเปลี่ยนแปลงปัจจุบัน

d.5 ความสัมฤทธิผลของมาตรการที่ได้ลงมือปฏิบัติไปแล้ว

d.6 เหตุการณ์ภายนอก ได้แก่ การเปลี่ยนแปลงที่มีต่อกฎระเบียบ กฎหมาย ข้อกำหนดในสัญญาที่ทำไว้ หรือข้อกำหนดอื่นๆ และการเปลี่ยนแปลงทางสังคม เป็นต้น

e) ดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยภายในองค์กรตามรอบระยะเวลาที่ได้กำหนดไว้ (ดูข้อ 3)

f) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหารอย่างสม่ำเสมอ (ดูข้อ 4.1)

g) ปรับปรุงแผนทางด้านความมั่นคงปลอดภัยโดยนำผลของการเฝ้าระวังและทบทวนกิจกรรมต่างๆ มาพิจารณาร่วมด้วย

h) บันทึกการดำเนินการซึ่งอาจมีผลกระทบต่อความสัมฤทธิผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัย (ดูข้อ 1.3.3)

1.2.4 บำรุงรักษาและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย องค์กรควรปฏิบัติดังนี้ (Act)

a) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยตามที่ระบุไว้

b) ใช้มาตรการเชิงแก้ไขและป้องกันตามข้อ 5.2 และ 5.3 และใช้บทเรียนจากประสบการณ์ทางด้านความมั่นคงปลอดภัยขององค์กรเองและขององค์กรอื่นมาช่วยในการปรับปรุงให้ดีขึ้น
c) แจ้งการปรับปรุงและการดำเนินการให้แก่ทุกหน่วยที่เกี่ยวข้อง โดยให้รายละเอียดที่เหมาะสมต่อสถานการณ์ที่เกิดขึ้น
d) ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

1.3 ข้อกำหนดทางด้านการจัดทำเอกสาร

1.3.1 ความต้องการทั่วไป

เอกสารที่จำเป็นต้องจัดทำจะรวมถึงบันทึกแสดงการตัดสินใจของผู้บริหาร เอกสารจะต้องประกอบด้วย

a) นโยบายความมั่นคงปลอดภัยตามข้อ 1.2.1 b และวัตถุประสงค์
b) ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัย
c) ขั้นตอนการปฏิบัติและมาตรการสนับสนุนระบบบริหารจัดการความมั่นคงปลอดภัย
d) วิธีการประเมินความเสี่ยง ตามข้อ 1.2.1 c
e) รายงานการประเมินความเสี่ยง ตามข้อ 1.2.1 c to 1.2.1 g
f) แผนการจัดการความเสี่ยงตามข้อ 1.2.2 b
g) ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการวางแผน การดำเนินการและการควบคุมกระบวนการทางด้านความมั่นคงปลอดภัย รวมทั้งวิธีการวัดความสัมฤทธิผลของมาตรการตามข้อ 1.2.3 c
h) สิ่งที่ต้องบันทึกไว้ ซึ่งกำหนดโดยมาตรฐานนี้ (ดูข้อ 1.3.3)
i) เอกสารแสดงการใช้งานมาตรการ หรือ Statement of Aplicability (SoA)

1.3.2 การบริหารจัดการเอกสาร

เอกสารตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัย จะต้องได้รับการป้องกันและควบคุม ขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการจัดการเอกสาร ควรมีขั้นตอนที่เกี่ยวข้อง ดังนี้

a) อนุมัติการใช้งานเอกสารก่อนที่จะเผยแพร่
b) ทบทวน ปรับปรุง และอนุมัติเอกสารตามความจำเป็น
c) ระบุการเปลี่ยนแปลงและสถานภาพของเอกสารปัจจุบัน
d) กำหนดเลขที่เอกสารตามการปรับปรุงที่เกิดขึ้น
e) จัดทำให้เอกสารสามารถอ่าน ทำความเข้าใจ และระบุได้โดยง่าย
f) จัดทำให้เอกสารสามารถเข้าถึงได้เฉพาะผู้ที่มีความจำเป็นในการใช้งาน รวมทั้งการโอนย้าย การจัดเก็บ และการทำลายเอกสารจะต้องเป็นไปตามขั้นตอนปฏิบัติที่จัดทำไว้สำหรับเอกสารชนิดนั้น
g) สามารถระบุได้ว่าเอกสารใดเป็นเอกสารจากภายนอก
h) ควบคุมการแจกจ่ายหรือการเผยแพร่เอกสาร
i) ป้องกันการใช้เอกสารล้าสมัย (หรือเลิกใช้งานแล้ว)
j) ใช้วิธีการระบุเอกสารที่เหมาะสมหากเอกสารล้าสมัยนั้นยังคงเก็บไว้เพื่อจุดประสงค์ใดจุดประสงค์หนึ่ง

1.3.3 การบริหารจัดการบันทึกข้อมูล หรือฟอร์มต่างๆ

องค์กรจะต้องมีการกำหนด จัดทำ และบำรุงรักษาบันทึกข้อมูลหรือฟอร์มต่างๆ เพื่อใช้เป็นหลักฐานแสดงความสอดคล้องกับข้อกำหนดและการดำเนินการที่มีประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยบันทึกข้อมูลที่เก็บไว้จะสะท้อนถึงประสิทธิภาพของกระบวนการตามหัวข้อ 1.2 และการเกิดขึ้นของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ทั้งนี้ บันทึกข้อมูลหรือฟอร์มต่างๆ จะต้อง

- ได้รับการป้องกันและควบคุม

- จัดเก็บไว้ในกรณีที่เป็นบันทึกข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางด้านกฎหมาย หรือระเบียบ หรือที่ระบุไว้ในสัญญาและนโยบายความมั่นคงปลอดภัย
- สามารถอ่านทำความเข้าใจ ระบุ และนำขึ้นมาใช้งานได้โดยง่าย
- ได้รับการกำหนดมาตรการที่จำเป็นสำหรับการกรอกหรือบันทึก การจัดเก็บ การป้องกัน การนำขึ้นมาใช้งาน ระยะเวลาที่จะต้องจัดเก็บไว้และการทำลายบันทึกข้อมูล และมาตรการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษร และมีการนำไปปฏิบัติจริง

ข้อ 2 หน้าที่ความรับผิดชอบของผู้บริหาร

2.1 การให้ความสำคัญในการบริหารจัดการ

ผู้บริหารจะต้องแสดงถึงการให้ความสำคัญต่อการกำหนดการลงมือปฏิบัติการ ดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษาและการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยโดย

a) กำหนดนโยบายความมั่นคงปลอดภัย
b) กำหนดวัตถุประสงค์และแผนสำหรับระบบบริหารจัดการ
c) กำหนดบทบาทและหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย
d) แจ้งทุกหน่วยภายในองค์กรได้รับทราบถึงความสำคัญของการรักษาความมั่นคงปลอดภัยและการปฏิบัติตามนโยบายความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบภายใต้กฎหมายของประเทศ รวมทั้งการยกระดับทางด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง
e) จัดสรรทรัพยากรอย่างพอเพียงสำหรับการกำหนด การลงมือปฏิบัติการดำเนินการ การเฝ้าระวัง การทบทวน การบำรุงรักษา และการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย (ดูข้อ 2.2.1)
f) กำหนดเกณฑ์ในการยอมรับความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้
g) จัดให้มีการตรวจสอบภายในสำหรับระบบบริหารจัดการความมั่นคงปลอดภัย
h) ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัย

2.2 การบริหารจัดการทรัพยากร

2.2.1 การจัดสรรทรัพยากร

องค์กรจะต้องจัดสรรทรัพยากรที่จำเป็นเพื่อ

a) กำหนด ลงมือปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน บำรุงรักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย
b) ให้มีการดำเนินการตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัย
c) ให้สามารถระบุข้อกำหนดที่เกี่ยวข้องกับกฎหมายและระเบียบปฏิบัติ รวมถึงข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้ในสัญญา
d) ให้สามารถบำรุงรักษาความมั่นคงปลอดภัยอย่างพอเพียง โดยการเลือกใช้มาตรการทางด้านความมั่นคงปลอดภัยที่ถูกต้องและเหมาะสม
e) ให้มีการดำเนินการทบทวนตามความจำเป็น รวมถึงมีการดำเนินการเพิ่มเติมอย่างเหมาะสมต่อผลของการทบทวนนั้น
f) ให้สามารถปรับปรุงความสัมฤทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัย

2.2.2 การอบรม การสร้างความตระหนัก และการเพิ่มขีดความสามารถ

องค์กรจะต้องดำเนินการเพื่อให้บุคลากรทั้งหมดที่ได้รับมอบหมายหน้าที่ความรับผิดชอบตามที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัย บุคลากรเหล่านั้นควรมีขีดความสามารถที่จะปฏิบัติงานตามที่กำหนดไว้ ดังนี้

a) กำหนดความรู้ความสามารถที่จำเป็นสำหรับบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัย
b) จัดการอบรมหรือใช้วิธีการอื่น (เช่น ว่าจ้างบุคลากรที่มีความสามารถ) เพื่อเป็นการเสริมความรู้ความสามารถ
c) ประเมินความสัมฤทธิผลของการดำเนินการในข้อ b)

d) เก็บรักษาบันทึกข้อมูลที่เกี่ยวข้องกับการศึกษา การฝึกอบรม ทักษะ ประสบการณ์และคุณสมบัติของบุคลากรขององค์กร (การเก็บประวัติการเข้ารับการอบรมของบุคลากร จัดเก็บเป็นหลักฐานสำหรับการตรวจสอบด้วยข้อ 1.3.3)

องค์กรจะต้องดำเนินการให้บุคลากรที่เกี่ยวข้องมีความตระหนักถึงความเกี่ยวข้องและความสำคัญของกิจกรรมทางด้านความมั่นคงปลอดภัยที่บุคคลเหล่านี้เป็นส่วนหนึ่งและมีผลต่อความสำเร็จของระบบบริหารจัดการความมั่นคงปลอดภัย

ข้อ 3 การตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัย

องค์กรควรดำเนินการตรวจสอบภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัย

a) สอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องหรือไม่
b) สอดคล้องกับข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือไม่
c) ได้รับการลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิผลหรือไม่
d) เป็นไปตามที่คาดหมายไว้หรือไม่

องค์กรจะต้องวางแผนตรวจสอบภายในโดยพิจารณาถึงสถานภาพและความสำคัญของกระบวนการและส่วนต่างๆ ที่จะได้รับการตรวจสอบ รวมทั้งผลการตรวจสอบจากครั้งต่างๆ ที่ผ่านมา องค์กรจะต้องกำหนดเกณฑ์ในการตรวจสอบ ขอบเขต ความถี่ และวิธีการที่ใช้ในการตรวจสอบ การคัดเลือกผู้ตรวจสอบ และการดำเนินการตรวจสอบจะต้องคำนึงถึงหลักฐานตามความเป็นจริง และความเที่ยงธรรมของผู้ตรวจสอบ รวมทั้งผู้ตรวจสอบจะต้องไม่ตรวจสอบงานของตนเอง

องค์กรต้องระบุหน้าที่ความรับผิดชอบและข้อกำหนดต่างๆ ในการวางแผนและดำเนินการตรวจสอบ รวมทั้งการจัดทำรายงานผลการตรวจสอบ และบำรุงรักษาบันทึกข้อมูลที่เกี่ยวข้องกับการตรวจสอบนั้น (ดูข้อ 1.3.3) อย่างเป็นลายลักษณ์อักษร

ผู้บริหารที่รับผิดชอบในส่วนที่ได้รับการตรวจสอบจะต้องควบคุมให้การดำเนินการแก้ไขเพื่อกำจัดความไม่สอดคล้องและสาเหตุที่เกี่ยวข้องได้รับการดำเนินการโดยปราศจากความล่าช้าที่เกินควร รวมทั้งจะต้องควบคุมให้มีกิจกรรมการติดตามเพื่อตรวจสอบการดำเนินการที่ได้ดำเนินการไปแล้ว และมีการจัดทำรายงานผลการตรวจสอบนั้น (ดูข้อ 5)

ข้อ 4 การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร

4.1 ข้อกำหนดทั่วไป

ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่น ปีละ 1 ครั้ง) เพื่อให้มีการดำเนินการที่เหมาะสม พอเพียงและสัมฤทธิผล การทบทวนจะต้องรวมถึงการปรับปรุงหรือเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัย ซึ่งหมายรวมถึงนโยบายความมั่นคงปลอดภัยและวัตถุประสงค์ทางด้านความมั่นคงปลอดภัย ผลของการทบทวนจะต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษรและบันทึกข้อมูลที่เกี่ยวข้องกับการทบทวนจะต้องได้รับการบำรุงรักษาไว้ (ดูข้อ 1.3.3)

4.2 ข้อมูลนำเข้าที่ใช้ในการทบทวน

ข้อมูลนำเข้าที่ใช้ในการทบทวนโดยผู้บริหารจะรวมถึง

a) ผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยและผลการทบทวน
b) ผลตอบกลับจากทุกหน่วยที่เกี่ยวข้อง
c) เทคนิค ผลิตภัณฑ์ หรือขั้นตอนปฏิบัติซึ่งสามารถใช้ในการปรับปรุงประสิทธิภาพและความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย
d) สถานภาพของการดำเนินการเชิงป้องกันและการดำเนินการเชิงแก้ไข
e) จุดอ่อนหรือภัยคุกคามที่ยังไม่ได้รับการกล่าวถึงในรายงานการประเมินความเสี่ยงครั้งที่ผ่านมา

f) ผลของการวัดความสัมฤทธิผล

g) การดำเนินการติดตามจากผลการทบทวนครั้งต่างๆ ที่ผ่านมา

h) การเปลี่ยนแปลงแก้ไขที่อาจมีผลต่อระบบบริหารจัดการความมั่นคงปลอดภัย

i) ข้อเสนอแนะในการปรับปรุงแก้ไข

4.3 ผลจากการทบทวน

ผลจากการทบทวนโดยผู้บริหารจะรวมถึงการตัดสินใจและการดำเนินการต่างๆ ดังนี้

a) การปรับปรุงทางด้านความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัย

b) การปรับปรุงด้านการประเมินความเสี่ยงและปรับปรุงแผนการจัดการกับความเสี่ยง

c) การแก้ไขขั้นตอนปฏิบัติและมาตรการที่มีผลต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ การแก้ไขดังกล่าวอาจเป็นผลมาจากการเปลี่ยนแปลงดังนี้

c.1 ข้อกำหนดทางธุรกิจ

c.2 ข้อกำหนดทางด้านความมั่นคงปลอดภัย

c.3 กระบวนการทางธุรกิจที่มีผลต่อข้อกำหนดทางธุรกิจที่มีอยู่ในปัจจุบัน

c.4 ข้อกำหนดที่เกี่ยวข้องกับกฎ ระเบียบ หรือกฎหมาย

c.5 ข้อกำหนดที่ระบุไว้ในสัญญา

c.6 ระดับของความเสี่ยง และ/หรือเกณฑ์สำหรับการยอมรับความเสี่ยง

d) ความต้องการด้านทรัพยากร

e) การปรับปรุงวิธีการวัดความสัมฤทธิผลของมาตรการที่ใช้

ข้อ 5 การดำเนินการเพื่อบำรุงรักษาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย

5.1 การปรับปรุงอย่างต่อเนื่อง

องค์กรจะต้องปรับปรุงความสัมฤทธิผลของระบบบริหารความมั่นคงปลอดภัยอย่างต่อเนื่องโดยใช้

- นโยบายความมั่นคงปลอดภัย
- วัตถุประสงค์ทางด้านความมั่นคงปลอดภัย
- ผลการตรวจสอบความมั่นคงปลอดภัย
- ผลการวิเคราะห์เหตุการณ์ที่ได้รับการเฝ้าระวัง
- การดำเนินการเชิงแก้ไขและป้องกัน
- การทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยโดยผู้บริหาร

5.2 การดำเนินการเชิงแก้ไข

องค์กรจะดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนดสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยเพื่อป้องกันการเกิดขึ้นอีก ขั้นตอนปฏิบัติสำหรับการดำเนินการเชิงแก้ไขที่เป็นลายลักษณ์อักษรจะต้องพิจารณาถึง

a) การระบุความไม่สอดคล้อง
b) การระบุสาเหตุของความไม่สอดคล้อง
c) การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันไม่ให้ความไม่สอดคล้องนั้นเกิดขึ้นอีก
d) การลงมือปฏิบัติการดำเนินการเชิงแก้ไขตามความจำเป็น
e) การบันทึกข้อมูลผลการดำเนินการ (ดูข้อ 1.3.3)
f) การทบทวนการดำเนินการเชิงแก้ไขที่ได้ปฏิบัติไปแล้ว

5.3 การดำเนินการเชิงป้องกัน

องค์กรจะต้องดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนดสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยที่มีโอกาสเกิดขึ้นเพื่อป้องกันการเกิดขึ้น

การดำเนินการเชิงป้องกันจะต้องเหมาะสมกับผลกระทบของปัญหาที่มีโอกาสเกิดขึ้น ขั้นตอนปฏิบัติสำหรับการดำเนินการเชิงป้องกันที่เป็นลายลักษณ์อักษรจะต้องพิจารณาถึง

a) การระบุความไม่สอดคล้องที่มีโอกาสเกิดขึ้นและสาเหตุของความไม่สอดคล้อง
b) การประเมินความจำเป็นในการดำเนินการเพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้อง
c) การลงมือปฏิบัติการดำเนินการเชิงป้องกันตามความจำเป็น
d) การบันทึกข้อมูลผลการดำเนินการ (ดูข้อ 1.3.3)
e) การทบทวนการดำเนินการเชิงป้องกันที่ได้ปฏิบัติไปแล้ว

องค์กรจะต้องระบุความเสี่ยงที่แปรเปลี่ยนไปและกำหนดการดำเนินการเชิงป้องกัน โดยให้ความสำคัญกับความเสี่ยงที่มีระดับสูง รวมทั้งกำหนดลำดับความสำคัญของการดำเนินการเชิงป้องกัน โดยพิจารณาจากผลของการประเมินความเสี่ยง

ส่วนที่ 2

มาตรการการจัดการความมั่นคงปลอดภัย
สำหรับสารสนเทศ
(อ้างอิงตามมาตรฐาน ISO/IEC 27001 Annex A
และศึกษารายละเอียดวิธีปฏิบัติทางเทคนิค
จาก ISO/IEC 17799:2005)

มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ

1. นโยบายความมั่นคงปลอดภัย (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

(ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งานและต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)

(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization)

มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)

(ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)

(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการสัญญาว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)

(ผู้บริหารสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

(ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม

2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)

มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)

(หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

3. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)

มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศตามที่กำหนดไว้ในบัญชีทรัพย์สิน

3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแล และเอาใจใส่ เป็นต้น

3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)

มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมายและระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาท และหน้าที่

ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคล หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึงประกอบการคัดเลือกด้วย

4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้

และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)

(ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการ จ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)

(หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)

(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบาย หรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)

(หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)

(หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)

(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุมตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

5.1.2 การควบคุมการเข้า-ออก (Physical entry controls)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)

(หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงาน ในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

(พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น

5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

(ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาตหรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าว

ถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ

6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้ เป็นต้น

6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)

(หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

6.3.2 การตรวจรับระบบ (System acceptance)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)

มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)

(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

6.5 การสำรองข้อมูล (Back-up)

มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

6.5.1 การสำรองข้อมูล (Information back-up)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือค่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

6.6.1 มาตรการทางเครือข่าย (Network controls)

(ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)

มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)

(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กรอย่างเป็นลายลักษณ์อักษร

6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)

(หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่ายการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

7. การควบคุมการเข้าถึง (Access control)

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ

7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.1 การลงทะเบียนพนักงาน (User registration)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปหรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

7.2.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

(ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

7.3.1 การใช้งานรหัสผ่าน (Password use)

(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)

(พนักงาน) ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)

(ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

(ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)

(ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

(ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอปพลิเคชันที่ใช้งานทางธุรกิจได้ระบุไว้

7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

(ผู้ดูแลระบบ) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

(ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

(ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

7.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

(ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

(ผู้ดูแลระบบ) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

(ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

7.6 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and information access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอปพลิเคชันโดยไม่ได้รับอนุญาต

7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

(ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอปพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

(หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(ผู้บริหารสนเทศ) ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)

มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)

(ผู้พัฒนา และผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

8.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (Correct processing in applications)

มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอปพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)

(ผู้พัฒนาระบบ) ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอปพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร

8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้บริการ

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)

(ผู้พัฒนาระบบ) ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ

8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)

(หัวหน้างานสารสนเทศ) ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.5.2 การตรวจสอบการทำงานของแอปพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

(ผู้ดูแลระบบ) ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอปพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)

(หัวหน้างานสารสนเทศ) ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป

8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้ง กำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)

(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)

มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ

กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)

(หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)

(ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ

10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

11. การปฏิบัติตามข้อกำหนด (Compliance)

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

(หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP))

(หัวหน้างานนิติการ) ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย

11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)

(หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง

11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)

(หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)

มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)

มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน

11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

ภาคผนวก ก

คำนิยาม

"พนักงาน" หมายความว่า พนักงานและลูกจ้างที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบภายในองค์กร

"ผู้บริหารองค์กร" หมายความว่า พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร

"ผู้บริหารสารสนเทศ" หมายความว่า พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในองค์กร

"ผู้ดูแลระบบ" หมายความว่า พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

"หัวหน้างานสารสนเทศ" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

"หัวหน้างานบุคคล" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการวางแผนทรัพยากรบุคคลทั้งคุณภาพ ปริมาณและสัดส่วนให้มีความเหมาะสมกับภารกิจ และแผนกลยุทธ์ของหน่วยงาน

ระดับต่างๆ ทั้งในระยะสั้นและระยะยาว รวมถึงบริหารทรัพยากรบุคคลตามระเบียบ/หลักเกณฑ์ของสำนักงาน

"หัวหน้างานอาคาร" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลและบริหารจัดการระบบสาธารณูปโภคต่างๆ และทรัพยากรสิ่งอำนวยความสะดวกภายในอาคาร รวมถึงดูแลความเป็นระเบียบเรียบร้อยและการรักษาความปลอดภัยของสำนักงาน

"หัวหน้างานธุรการ" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลเกี่ยวกับงานธุรการและสารบรรณภายในองค์กร

"หน่วยงานภายนอก" หมายความว่า องค์กรอื่นๆ ที่เกี่ยวข้อง เช่น บริษัทขายฮาร์ดแวร์หรือซอฟต์แวร์ บริษัทให้คำปรึกษาเกี่ยวกับระบบสารสนเทศ เป็นต้น

"หัวหน้างานนิติการ" หมายความว่า พนักงานที่มีหน้าที่ให้ความคิดเห็นหรือตีความเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมาย พระราชบัญญัติ กฤษฎีกา หรือข้อความในเชิงระเบียบข้อบังคับอื่นๆ รวมทั้งจัดทำระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ หรือคำสั่งสำหรับใช้ในองค์กร

เกณฑ์การประเมินหน่วยงานที่เข้าข่าย Critical Infrastructure สำหรับประเทศไทย

ด้านมูลค่าความเสียหาย

☆ = เสียหายทางธุรกิจมูลค่าประมาณ 1 ล้านบาท ต่อวัน

☆☆ = เสียหายทางธุรกิจมูลค่าระหว่าง 1 - 100 ล้านบาท ต่อวัน

☆☆☆ = เสียหายทางธุรกิจมูลค่าเกินกว่า 100 ล้านบาท ต่อวัน

ด้านผู้ใช้ที่ได้รับผลกระทบ

☆ = กระทบผู้ใช้จำนวนประมาณน้อยกว่า 10,000 คน

☆☆ = กระทบผู้ใช้จำนวนประมาณ 10,000 - 100,000 คน

☆☆☆ = กระทบผู้ใช้จำนวนประมาณมากกว่า 100,000 คน

ด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน

☆ = ไม่ได้รับผลกระทบต่อชีวิตและสุขภาพ

☆☆ = หากบาดเจ็บหรือป่วย 1 คน

☆☆☆ = หากเสียชีวิตเพียง 1 คน

ด้านผลกระทบต่อความมั่นคงและความสงบเรียบร้อยของสังคม ประเมินเป็น 2 ค่าคือ

0 = ไม่มีผลกระทบ

1 = มีผลกระทบ

หมายเหตุ มูลค่าความเสียหาย หมายถึง มูลค่าเงินโดยรวมที่คำนวณขึ้นจากความเสียหายตรงหน้า (Incidental Damage) เมื่อบริการที่หน่วยงานหรือองค์กร ภาครัฐนั้น หยุดให้บริการไปในช่วงเวลาหนึ่ง

ภาคผนวก ข

ด่วนมาก
ที่ นร ๐๕๐๖/๖๓๔/๒๙

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๑๔ พฤศจิกายน ๒๕๔๙

เรื่อง แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรียน รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

อ้างถึง หนังสือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ทก ๐๒๐๐.๑๑ (ปคร)/๖๑๐๘ ลงวันที่ ๖ พฤศจิกายน ๒๕๔๙

สิ่งที่ส่งมาด้วย สำเนาประกาศสำนักนายกรัฐมนตรี

ตามที่ได้ขอให้นำเสนอคณะรัฐมนตรีพิจารณาแต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ความละเอียดแจ้งแล้ว นั้น

คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๗ พฤศจิกายน ๒๕๔๙ อนุมัติให้แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน ๑๒ คน โดยให้มีผลตั้งแต่วันที่คณะรัฐมนตรีมีมติเป็นต้นไป ดังนี้

๑. ด้านการเงิน
ภาครัฐ นายฉิม ตันติยาสวัสดิกุล
ภาคเอกชน นายชาติศิริ โสภณพนิช

๒. ด้านพาณิชย์อิเล็กทรอนิกส์
ภาครัฐ นางสาวชุติมา บุณยประภัศร
ภาคเอกชน พลเรือตรี ประสาท ศรีผดุง

๓. ด้านนิติศาสตร์
ภาครัฐ นายพิบัย ณ นคร
ภาคเอกชน นายชวลิต อัตถศาสตร์

๔. ด้านวิทยาการคอมพิวเตอร์
ภาครัฐ นางชนนุช ตรีทิพยบุตร
ภาคเอกชน นายยงยศ พรตปกรณ์

๕. ด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์
ภาครัฐ นายเวีศักดิ์ กออนันตกูล
ภาคเอกชน นายชาลิต ทิสยากร

๖. ด้านสังคมศาสตร์
ภาครัฐ นายอาณัติ สีมัคเดช
ภาคเอกชน นายยงสิทธิ์ โรจน์ศรีวิชัยกุล

สำนักเลขาธิการคณะรัฐมนตรีได้จัดทำประกาศสำนักนายกรัฐมนตรีในเรื่องนี้เสร็จเรียบร้อยแล้ว ตามสำเนาประกาศสำนักนายกรัฐมนตรีที่ส่งมาด้วยนี้

จึงเรียนยืนยันมา และขอได้โปรดแจ้งให้ผู้ที่ได้รับการแต่งตั้งทราบต่อไปด้วย

ขอแสดงความนับถือ

(นางสาวสิบหัน วนวิสุทธิ์)
ผู้อำนวยการสำนักวิเคราะห์เรื่องเสนอคณะรัฐมนตรี ปฏิบัติราชการแทน
เลขาธิการคณะรัฐมนตรี

สำนักวิเคราะห์เรื่องเสนอคณะรัฐมนตรี
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๓๒๔
โทรสาร ๐ ๒๒๘๐ ๙๑๖๔
www.cabinet.thaigov.go.th
(๓๔๑_๑๑_๓๐รายงานโนต)

คณะผู้จัดทำ

ที่ปรึกษา

1. ดร. ทวีศักดิ์ กออนันตกูล
   รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
2. ดร. พันธ์ศักดิ์ ศิริรัชตพงษ์
   ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
3. ดร. ชฎามาศ ธุวะเศรษฐกุล
   รองผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
4. นางสุรางคณา วายุภาพ
   หัวหน้าสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
   ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
5. ดร. ศิวรักษ์ ศิวโมกษธรรม
   หัวหน้าหน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคง
   ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

รายนามผู้ศึกษาและเรียบเรียง

1. ดร. โกเมน พิบูลย์โรจน์
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
2. ดร. บรรจง หะรังษี
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
3. น.ส. ดวงกมล ทรัพย์พิทยากร
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
4. น.ส. ศิริวรรณ อภิสิริเดช
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
5. นายพุธ นาฑีสุวรรณ
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

6. น.ส.ภัทราวดี เหมทานนท์
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
7. น.ส.ธารทิพย์ ตากเทอดเกียรติ
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
8. นายเลอศักดิ์ ลิ้มวิวัฒน์กุล
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
9. นายชวลิต ทินกรสูติบุตร
   ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
10. นายปิยวัฒน์ เลื่อนสุขันธ์
    ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
11. นายไตรรัตน์ พุทธรักษา
    ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ออกแบบและจัดพิมพ์

1. น.ส. ลัญจนา นิตยพัฒน์
   สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
2. น.ส. ฉิทกา โกมารกุล ณ นคร
   สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ