<table>
<tr><td rowspan="2"> 
BOI</td><td colspan="2">คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
(ISMS Manual)</td></tr>
<tr><td>รหัสเอกสาร M IT SP 01-00 ชุดที่ 04</td><td>เริ่มใช้ 16/07/58</td></tr>
<tr><td>ผู้ทบทวน .....
นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
(ตำแหน่ง ทป-อ.)</td><td>ผู้อนุมัติ .....
นางหิรัญญา สุจินัย
(ตำแหน่ง ลกท.)</td><td>หน้าที่ 1 ของ 27</td></tr>
</table>

สารบัญ

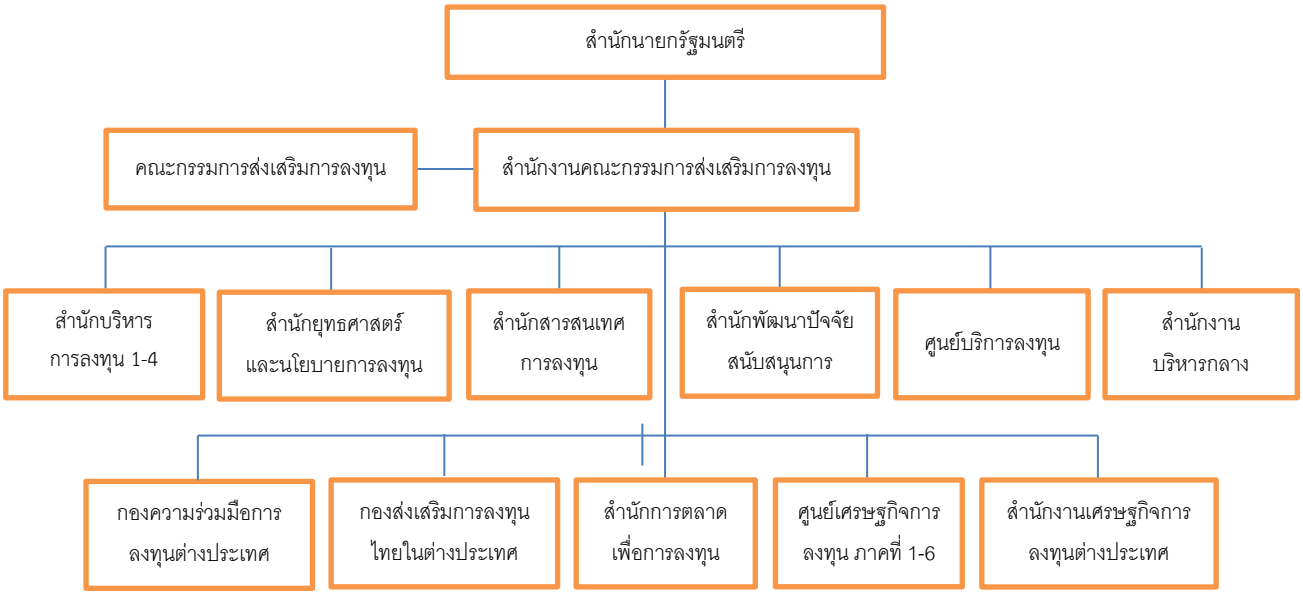
1. บทนำ

สำนักงานคณะกรรมการส่งเสริมการลงทุนเป็นส่วนราชการในสังกัดสำนักนายกรัฐมนตรี มีภารกิจในการส่งเสริมให้เกิดการลงทุนในกิจการที่เป็นประโยชน์ต่อประเทศโดยการให้สิทธิและประโยชน์ในการลงทุนการเสริมสร้างปัจจัยเกื้อหนุนต่อการลงทุนการส่งเสริมการลงทุนและการบริการลงทุนเพื่อเสริมสร้างความเข้มแข็งให้กับระบบเศรษฐกิจและสังคมโดยรวมของประเทศโดยให้มีอำนาจหน้าที่ดังต่อไปนี้

1) ดำเนินการตามกฎหมายว่าด้วยการส่งเสริมการลงทุนและกฎหมายอื่นที่เกี่ยวข้อง
2) ปฏิบัติตามมติของคณะกรรมการส่งเสริมการลงทุนหรือตามที่คณะกรรมการส่งเสริมการลงทุนมอบหมาย
3) ดำเนินการโฆษณาเผยแพร่บรรยากาศการลงทุนและชักจูงให้มีการลงทุนในกิจการที่สำคัญและเป็นประโยชน์ในด้านเศรษฐกิจสังคมและความมั่นคงของประเทศ
4) จัดให้มีศูนย์บริการลงทุนสำหรับผู้สนใจลงทุนและผู้ลงทุนในการจัดให้ได้มาซึ่งการอนุญาตและการให้ใช้บริการต่าง ๆ ที่เกี่ยวกับการลงทุนซึ่งรวมถึงการอำนวยความสะดวกและให้ความช่วยเหลือแก่ผู้สนใจลงทุนในการเตรียมโครงการลงทุนการหาผู้ร่วมลงทุนและดำเนินการตามโครงการลงทุนศึกษาลู่ทางในการลงทุนและวางแผนส่งเสริมการลงทุนรวมทั้งประสานการแก้ไขปัญหานักลงทุน
5) วิเคราะห์โครงการการขอรับการส่งเสริมการลงทุนตรวจสอบและควบคุมตลอดจนประเมินผลการลงทุนตามโครงการที่ได้รับการส่งเสริมการลงทุน
6) ศึกษาค้นคว้าหาลู่ทางในการลงทุนจัดทำรายงานความเหมาะสมของการลงทุนและวางแผนส่งเสริมการลงทุน
7) ศึกษาและรวบรวมข้อมูลเกี่ยวกับการลงทุนในประเทศ
8) ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของสำนักงานหรือตามที่กระทรวงหรือคณะรัฐมนตรีมอบหมาย

สำนักงานคณะกรรมการส่งเสริมการลงทุนมีสำนักงานตั้งอยู่เลขที่ 555 ถนนวิภาวดี-รังสิต เขตจตุจักร กรุงเทพฯ 10900 โทรศัพท์ (66) 25538111 โทรสาร (66) 25538222 Homepage: http://www.boi.go.th
E-Mail: head@boi.go.th

การแบ่งส่วนราชการสำนักงานคณะกรรมการส่งเสริมการลงทุน



ภาพ 1 แผนภูมิการแบ่งส่วนราชการ

การรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security) เป็นเรื่องสำคัญสำหรับทุกองค์กร เพราะปัจจุบันองค์กรได้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนงานตามภารกิจต่าง ๆ และเพื่อบริการให้กับลูกค้า ส่งผลให้มีการปรับปรุงและพัฒนาให้เกิด ระบบข้อมูลสารสนเทศ องค์ความรู้และบริการใหม่ ๆ ที่ความสำคัญต่อธุรกิจและเป็นสินทรัพย์ที่มีค่าขององค์กร จากเหตุผลดังกล่าวกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะผู้ดูแลภาพรวมการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ ได้เห็นถึงความสำคัญเรื่องความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้มีการจัดทำแผนแม่บท ICT Security แห่งชาติขึ้นเพื่อกำหนดกรอบแนวทางให้องค์กรและหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน รวมถึงประชาชนทั่วไปนำไปใช้ โดยส่วนหนึ่งของแผนงานระบุว่าให้หน่วยงานภาครัฐมีการสร้างกระบวนงานและจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งแผนฉบับนี้อ้างอิง “ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2013”

สำนักงานคณะกรรมการส่งเสริมการลงทุน ได้เล็งเห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารของสำนักงานจึงได้จัดทำ“ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ” (Information Security Management System: ISMS) ของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุนสำนักงานคณะกรรมการส่งเสริมการลงทุนเพื่อให้บริการระบบสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัยสร้างความเชื่อมั่นในการให้บริการ รวมถึงภาพลักษณ์ที่ดีแก่ลูกค้าและเพื่อป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้ข้อมูลสารสนเทศมีความถูกต้อง มีการรักษาความลับ และมีความพร้อมให้บริการอยู่ในระดับที่เหมาะสม

คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual) ฉบับนี้ ถือเป็นส่วนหนึ่งของการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศสำหรับห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน สำนักงานคณะกรรมการส่งเสริมการลงทุนเพื่อให้บริการสารสนเทศและการสื่อสาร ซึ่งอ้างถึงระบบบริหารความมั่นคงปลอดภัยสารสนเทศในภาพรวม ตามมาตรฐาน ISO/IEC 27001:2013

2. ขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Scope of Information Security Management System)

สำนักงานคณะกรรมการส่งเสริมการลงทุน ได้ดำเนินการวิเคราะห์และประเมินเทคโนโลยีที่ใช้ของระบบที่มีความสำคัญต่อภารกิจและการบริการของสำนักงานฯ ได้แก่

- ระบบ Active Directory
- ระบบ Website BOI (www.boi.go.th)
- ระบบ e-Mail

โดยการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) จากการประเมินผลกระทบต่อการดำเนินงานและความเสี่ยงของระบบ Active Directory ระบบ Website BOI และระบบ e-Mail สามารถสรุปถึงโอกาสที่จะเกิดความเสี่ยง ผลกระทบ และแนวทางการจัดการในแต่ละกรณี ได้ดังนี้

ตาราง 2-1 สรุปผลการวิเคราะห์และประเมินผลกระทบต่อการดำเนินงาน

บริการหลัก	กิจกรรม				ลำดับความสำคัญ (Critical) (ใช่/ไม่ใช่)	เป้าหมายการบริหารความต่อเนื่อง (Business Continuity Objective)		
	ระบบไฟฟ้า	ระบบเครือข่ายภายใน	ระบบเครือข่ายภายนอก	เครื่องคอมพิวเตอร์แม่ข่าย		MTPD (ชม.)	RTO (ชม.)	RPO
ระบบบริหารจัดการทรัพยากรระบบ (Active Directory)	✓	✓	✓	✓	**Yes**	24	4	ระบบสามารถให้บริการได้
บริการข้อมูลข่าวสาร (website : www.boi.go.th)	✓	✓	✓	✓	**Yes**	24	4	ระบบสามารถให้บริการได้
บริการจดหมายอิเล็กทรอนิกส์ (E-Mail)	✓	✓	✓	✓	**Yes**	24	4	ระบบสามารถให้บริการได้

หมายเหตุ:

(1) MTPD (Maximum Tolerable Period of Disruption) หมายถึง ระยะเวลาสูงสุดที่สามารถหยุดดำเนินการได้

(2) RTO (Recovery Time Objective) หมายถึง ระยะเวลาที่ต้องการดำเนินการกู้คืนสู่ระดับการดำเนินงานขั้นต่ำที่สามารถยอมรับได้

(3) RPO (Recovery Point Objective) หมายถึง ระดับการดำเนินงานขั้นต่ำที่สามารถยอมรับได้

ประเด็นภายในและภายนอก (Internal and External issues and requirements)

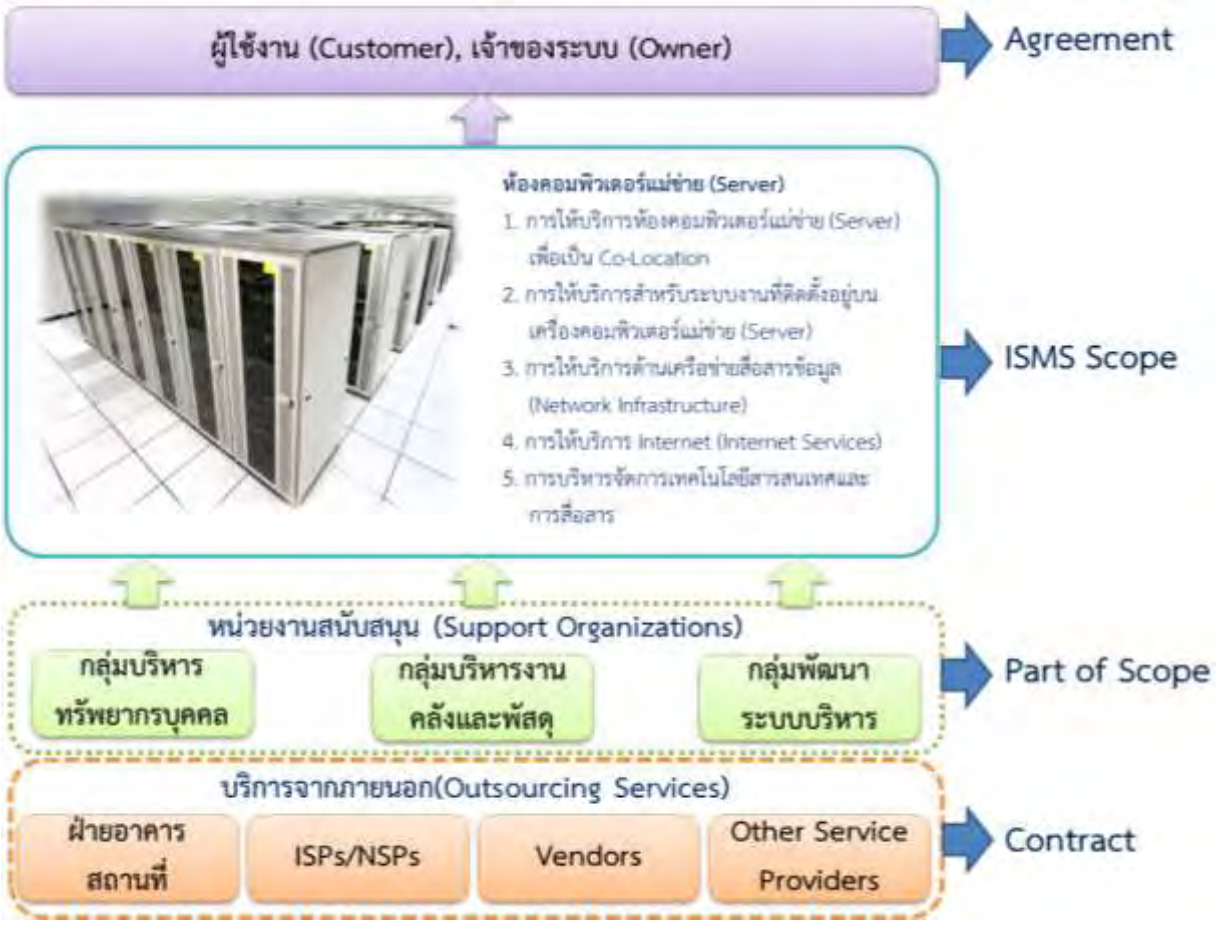
ประเด็นภายในและภายนอกที่เกี่ยวข้องกับขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) มีรายละเอียด ดังต่อไปนี้

ประเด็นภายใน		
ลำดับ	**ประเด็น**	**ผลกระทบ**
1	บุคลากรของสำนักงานฯ	- บุคลากรของสำนักงาน ฯ ไม่มีความรู้และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ - มีการเปลี่ยนแปลงบุคลากรของสำนักงานฯ บ่อยครั้ง ทำให้ขาดทักษะในการปฏิบัติงาน
2	นโยบายและกระบวนการปฏิบัติงาน	- นโยบายและกระบวนการปฏิบัติงานมีการเปลี่ยนแปลงบ่อยครั้ง - นโยบายและกระบวนการปฏิบัติงานไม่เอื้อในการรักษาความมั่นคงปลอดภัยสารสนเทศ
3	เทคโนโลยีสารสนเทศและการสื่อสาร	- มีการใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนการปฏิบัติงานจำนวนมาก - ระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความเกี่ยวข้องกันและมีความซับซ้อน
4	หน่วยงานราชการที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) และที่ปรึกษา กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)	- มีการรายงานผลการปฏิบัติงาน การใช้บริการและเชื่อมโยงข้อมูลกับหน่วยงานภายนอก อาจทำให้ข้อมูลความลับของสำนักงานฯ เปิดเผย หรือไม่ดำเนินการตามข้อตกลง
5	ผู้รับจ้าง เช่น บริษัทที่ปรึกษา ผู้ตรวจประเมิน ผู้รับจ้างบำรุงรักษาระบบ Hardware, Software, Network และ Security	- ผู้รับจ้างเปิดเผยข้อมูลความลับของสำนักงานฯ - ผู้รับจ้างไม่ดำเนินการตามสัญญา - ผู้รับจ้างสามารถเข้า-ออกสำนักงานได้ทั้งหมด

ประเด็นภายนอก		
ลำดับ	**ประเด็น**	**ผลกระทบ**
1	นักลงทุน/ผู้ประกอบการ	- มีนักลงทุน/ผู้ประกอบการติดต่อขอรับบริการจำนวนมาก และสามารถเข้า-ออกสำนักงานได้ทั้งหมด
2	การเมือง (Political)	- มีการปรับเปลี่ยนทางการเมืองบ่อยครั้ง - มีการเปลี่ยนแปลงโครงสร้างรัฐบาลบ่อยครั้ง - มีความขัดแย้ง การก่อการร้ายหรือการชุมนุมเกิดขึ้นบ่อยครั้ง
3	เศรษฐกิจ (Economic)	- การเปิดประชาคมเศรษฐกิจอาเซียน (AEC) ทำให้มีการติดต่อค้าขายกับประเทศสมาชิกอาเซียนมากขึ้น - แนวโน้มผลกระทบของการเปลี่ยนแปลงทางเทคโนโลยีหรืออื่นๆ ที่มีผลต่อเศรษฐกิจมีมากขึ้น
4	สังคมและวัฒนธรรม (Sociological)	- การใช้งานสื่อสังคมออนไลน์ที่มากขึ้น และมีความรวดเร็วมาก - สื่อโดยเฉพาะการนำเสนอข้อมูลข่าวที่เกี่ยวข้องกับองค์กรมีความรวดเร็วมากขึ้น - ทัศนคติทางสังคมและวัฒนธรรมมีการเปลี่ยนแปลงรวดเร็ว
5	เทคโนโลยี (Technological)	- การเปลี่ยนแปลงของเทคโนโลยีมีความรวดเร็วมาก - เทคโนโลยีที่สำนักงานฯ ใช้ในให้บริการจำเป็นต้องพัฒนาปรับปรุงอย่างต่อเนื่อง - นวัตกรรมทางเทคโนโลยี การประดิษฐ์ และการค้นพบใหม่ๆ ที่มากขึ้น - ความก้าวหน้าของอินเทอร์เน็ตและเครือข่ายการสื่อสารที่รวดเร็วมาก - ภัยคุกคามทางไซเบอร์ที่มากขึ้น
6	กฎหมาย (Legal)	- มีการบัญญัติและปรับปรุงกฎหมายด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง เช่น พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พรบ. คุ้มครองข้อมูลส่วนบุคคล ฯลฯ

ประเด็นภายนอก		
ลำดับ	**ประเด็น**	**ผลกระทบ**
7	สิ่งแวดล้อม (Environmental)	- ภาวะโลกร้อนทำให้เกิดภัยพิบัติรุนแรงขึ้น เช่น น้ำท่วม แผ่นดินไหว สึนามิ พายุ และ ไฟไม้ ฯลฯ - ระบบไฟฟ้าบริเวณสำนักงานฯ ดับบ่อย

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน สำนักงานคณะกรรมการส่งเสริมการลงทุน มีขอบเขตครอบคลุมเฉพาะการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งแสดงได้ตามภาพ 2



ภาพ 2 ภาพรวมขอบเขตระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)
ของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน
สำนักงานคณะกรรมการส่งเสริมการลงทุน

2.1 รายละเอียดขอบเขตระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน สำนักงานคณะกรรมการส่งเสริมการลงทุน ให้บริการระบบสารสนเทศและการสื่อสารครอบคลุมถึง

2.1.1 การให้บริการห้องคอมพิวเตอร์แม่ข่าย (Server) เพื่อเป็น Co-Location ดังนี้

- การบริการเชื่อมโยงเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Network Connectivity)
- การบริการเชื่อมโยง Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Internet Connectivity)
- การบริการสิ่งอำนวยความสะดวก (Facility Management)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (Security Management)
- การบริการดูแลช่วยเหลือ (Help Desk)

2.1.2 การให้บริการสำหรับระบบงานที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งประกอบไปด้วย

- การบริการสำรองข้อมูล (Backup & Restore)
- การบริการจัดการ Active Directory (AD)
- การจัดการเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ประกอบ (Hardware Management)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (Security Management)
- การบริการดูแลช่วยเหลือ (Help Desk)

2.1.3 การให้บริการด้านเครือข่ายสื่อสารข้อมูล (Network Infrastructure) ของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุนซึ่งประกอบไปด้วย

- การบริการเครือข่ายท้องถิ่น (Local Area Network: LAN)
- การบริการเครือข่ายทางไกล (Wide Area Network: WAN)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (Security Management)
- การบริการดูแลช่วยเหลือ (Help Desk)

2.1.4 การให้บริการ Internet (Internet Services) ของห้องคอมพิวเตอร์แม่ข่าย(Server) สำนักสารสนเทศการลงทุน ซึ่งประกอบไปด้วย

- การบริการเชื่อมโยง Internet
- การบริการระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- การบริการจัดการ Domain Name Service (DNS)
- การบริการเว็ปไซต์ (www.boi.go.th)
- การบริหารความมั่นคงปลอดภัยสารสนเทศ (Security Management)
- การบริการดูแลช่วยเหลือ (Help Desk)

2.1.5 การบริหารจัดการเทคโนโลยีสารสนเทศและการสื่อสารซึ่งดำเนินการภายในห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน ซึ่งประกอบไปด้วย

- การบริหารจัดการทรัพยากรบุคคลของหน่วยงานที่ดูแลการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- การจัดหาระบบ/ฮาร์ดแวร์/ซอฟต์แวร์/บริการ/และอุปกรณ์ประกอบอื่น ๆ เพื่อสนับสนุนการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่กล่าวมาข้างต้น

2.2 หน่วยงานและบุคลากรในขอบเขต

2.2.1 เจ้าหน้าที่ของสำนักสารสนเทศการลงทุน ซึ่งดูแลการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน

2.2.2 เจ้าหน้าที่ผู้ประสานงานกับกลุ่มบริหารทรัพยากรบุคคลซึ่งดูแลกระบวนการจัดการทรัพยากรบุคคลของสำนักสารสนเทศการลงทุน เพื่อสนับสนุนการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน

2.2.3 เจ้าหน้าที่ผู้ประสานงานกับกลุ่มบริหารงานคลังและพัสดุซึ่งดูแลกระบวนการจัดหาระบบ/ฮาร์ดแวร์/ซอฟต์แวร์/บริการ/และอุปกรณ์ประกอบอื่น ๆ เพื่อสนับสนุนการให้บริการระบบเทคโนโลยีสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน

2.2.4 เจ้าหน้าที่ของกลุ่มพัฒนาระบบบริหาร ซึ่งดูแลกระบวนการจัดการเอกสาร ISMS

2.2.5 เจ้าหน้าที่ผู้ประสานงานกับฝ่ายอาคารสถานที่ ซึ่งดูแลระบบสนับสนุนของห้องคอมพิวเตอร์แม่ข่าย อาทิ ระบบปรับอากาศและเครื่องกำเนิดไฟฟ้า

2.3 สถานที่ (Location)

ห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุน
สำนักงานคณะกรรมการส่งเสริมการลงทุน
555 ถ.วิภาวดีรังสิต เขตจตุจักร กรุงเทพฯ 10900
โทร (66) 2553 8220, (66) 2553 8111โทรสาร (66) 2553 8320

2.4 สินทรัพย์ที่อยู่ในขอบเขต (Asset)

สินทรัพย์ที่อยู่ในขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) จะประกอบด้วยข้อมูลซอฟต์แวร์ ฮาร์ดแวร์ การบริการ และบุคลากร ซึ่งครอบคลุมสินทรัพย์ที่สนับสนุนการให้บริการของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุนสำนักงานคณะกรรมการส่งเสริมการลงทุน

2.5 ข้อยกเว้น (Scope Excluded)

งานที่ไม่อยู่ในขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ(ISMS) ได้แก่ งานพัฒนาระบบสารสนเทศและงานนำเข้าและประมวลผลข้อมูลระบบสารสนเทศของผู้ใช้งาน

3. นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Policy Statement)

เป้าหมายของนโยบายเพื่อป้องกันสินทรัพย์สารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการให้บริการระบบสารสนเทศและการสื่อสารของห้องคอมพิวเตอร์แม่ข่าย (Server) สำนักสารสนเทศการลงทุนสำนักงานคณะกรรมการส่งเสริมการลงทุน จากภัยคุกคามภายในและภายนอกที่อาจเกิดขึ้นทั้งที่โดยเจตนาหรือไม่เจตนาก็ตาม

เพื่อแสดงถึงข้อผูกพันด้านคุณภาพและความมุ่งมั่นของสำนักงานคณะกรรมการส่งเสริมการลงทุนในการบริหารความมั่นคงปลอดภัยสารสนเทศ สำนักงานคณะกรรมการส่งเสริมการลงทุนจึงได้ประกาศนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ดังนี้

“การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร ห้องคอมพิวเตอร์แม่ข่าย ของสำนักงานคณะกรรมการส่งเสริมการลงทุนมีเสถียรภาพ มั่นคงปลอดภัย และสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013”

เพื่อให้บรรลุตามนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ดังกล่าว สำนักงานจะดำเนินการดังนี้

1. กำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) และให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่น ๆ ที่จำเป็นเพื่อให้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาและปรับปรุงอย่างต่อเนื่อง
2. แต่งตั้งผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative: ISMR) และคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อรับผิดชอบในการขับเคลื่อนและธำรงไว้ซึ่งระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
3. นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) ต้องสร้างความมั่นใจดังนี้
   - นโยบาย ขั้นตอน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ จะต้องถูกกำหนดและนำไปปฏิบัติอย่างเคร่งครัด เพื่อสนับสนุนนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)
   - ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการบูรณาการเข้ากับขั้นตอน และแนวทางปฏิบัติขององค์กร
   - สินทรัพย์สารสนเทศ จะต้องถูกรักษาสถานภาพด้านความลับ (Confidentiality) ด้านความถูกต้องสมบูรณ์ (Integrity) และด้านความพร้อมใช้งาน (Availability)
   - สินทรัพย์สารสนเทศ จะต้องถูกป้องกันจากผู้ไม่มีสิทธิในการเข้าถึง (Unauthorized access)

- มีการปฏิบัติตามคำสั่ง ระเบียบ ข้อบังคับ กฎหมาย และข้อตกลงที่มีผลต่อความมั่นคงปลอดภัย
- ทุกๆ เหตุการณ์ที่เกิดขึ้นที่มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศจะต้องถูกบันทึก ตรวจสอบ จัดการและรายงาน
- แผนบริหารความต่อเนื่องของธุรกิจจะต้องถูกพัฒนา ปรับปรุง และทดสอบ
- ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการตรวจสอบ การประเมิน และมีกระบวนการปรับปรุงอย่างต่อเนื่องให้เหมาะสมกับสถานการณ์ที่เปลี่ยนไป

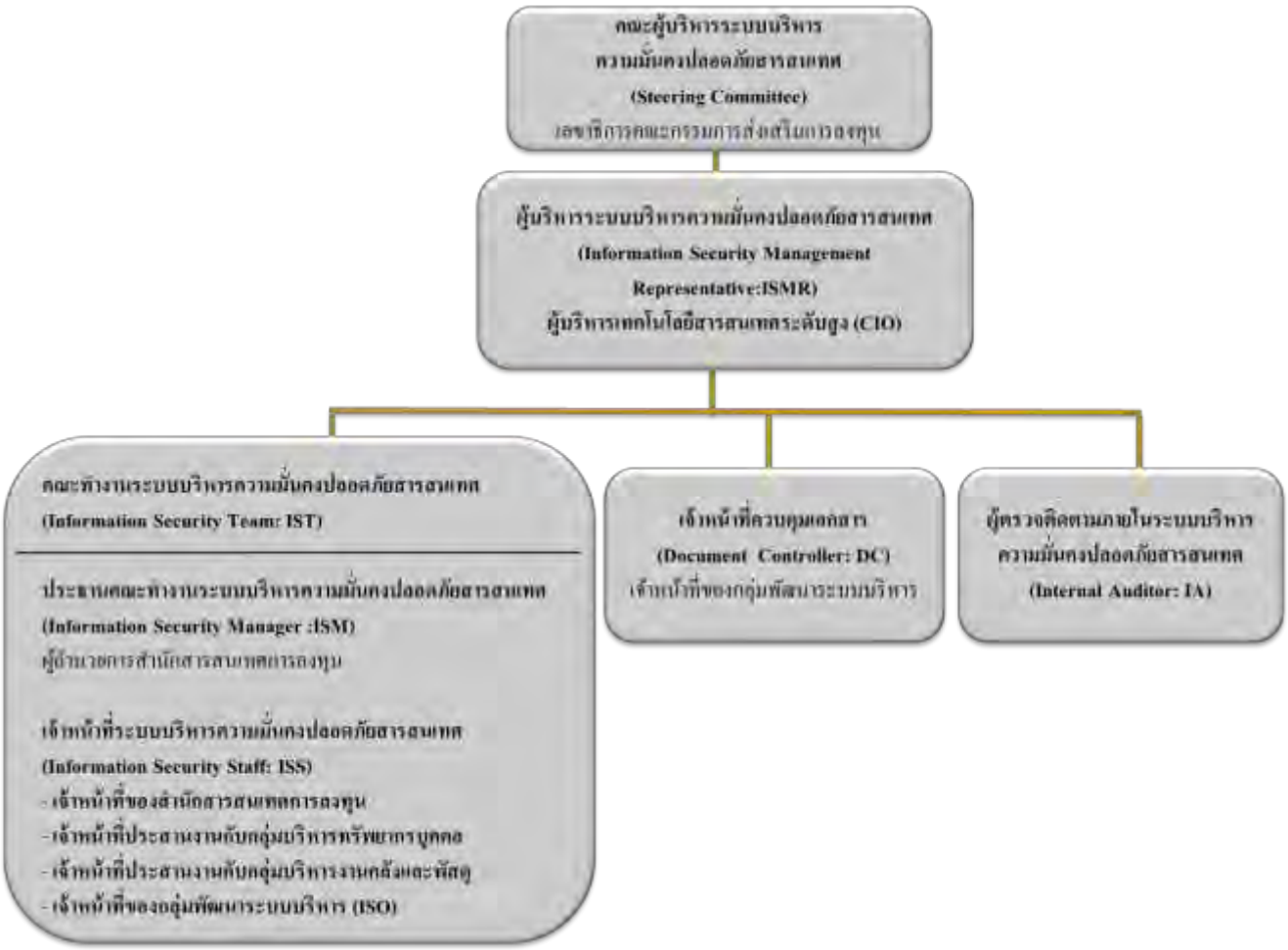
4. การบริหารความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการประเมิน และบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ตามคู่มือการบริหารจัดการความเสี่ยงสารสนเทศที่ได้รับการอนุมัติ

.....

เลขาธิการคณะกรรมการส่งเสริมการลงทุน

4. โครงสร้างคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Organization Structure)

โครงสร้างคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ของสำนักงานคณะกรรมการส่งเสริมการลงทุน ซึ่งแสดงได้ดังภาพ 3



ภาพ 3 โครงสร้างคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

โดยมีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

ตำแหน่ง	บทบาท หน้าที่ และความรับผิดชอบ
1. คณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee)	- สนับสนุนการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีการดำเนินงานอย่างต่อเนื่อง ตามมาตรฐาน ISO/IEC 27001:2013 - ทบทวนและอนุมัติขอบเขต แผนงาน และ นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) คู่มือการบริหารจัดการความเสี่ยง และอื่น ๆ ที่จำเป็น - สนับสนุนและอนุมัติงบประมาณด้านสารสนเทศ ทรัพยากร และองค์ประกอบอื่น ๆ ที่จำเป็นสำหรับการบริหารความมั่นคงปลอดภัยสารสนเทศ อย่างต่อเนื่อง - พิจารณารายงานด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Reports) ที่นำเสนอโดยผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) และดำเนินการตามความเหมาะสม - พิจารณาผลการตรวจสอบประเมินความเสี่ยง อนุมัติรายการความเสี่ยงที่คงเหลือ (Residual Risks) และอนุมัติแผนการบริหารความเสี่ยง (Risk Treatment Plan) - พิจารณาผลการตรวจติดตามภายใน (Internal ISMS Audit) - มอบหมายบทบาท หน้าที่และความรับผิดชอบให้ ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) ในการขับเคลื่อนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) การดำรงรักษาไว้ซึ่งระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) การติดตามและจัดทำรายงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) และอนุมัตินโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของ (ICT Security Policy) ขั้นตอน/แนวทางปฏิบัติ (Procedure/Guideline) และเอกสารต่าง ๆ ที่เกี่ยวข้องในการจัดทำและพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ตำแหน่ง	บทบาท หน้าที่ และความรับผิดชอบ
2. ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative: ISMR)	- ขับเคลื่อนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้ดำเนินการอย่างถูกต้องและดำรงรักษาไว้ซึ่งระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างต่อเนื่องตามมาตรฐาน ISO/IEC 27001:2013 - ติดตามผลการดำเนินการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) แก้ไขปัญหา และทบทวนรายงานด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Reports) อย่างต่อเนื่อง และนำเสนอต่อคณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่อทราบและพิจารณา - กำหนดให้แนวทาง กลยุทธ์ และมอบหมายหน้าที่ความรับผิดชอบในการดำเนินงานให้คณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Team: IST) เจ้าหน้าที่ควบคุมเอกสาร (Document Controller : DC) และผู้ตรวจติดตามภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Internal Auditor : IA) - กำกับดูแลให้เป็นไปตามนโยบายด้านการบริหารความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ - ทบทวนขอบเขต แผนงาน และ นโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) คู่มือการบริหารจัดการความเสี่ยง และอื่น ๆ ที่จำเป็น โดยจะต้องมีการทบทวนและอนุมัติ ให้อย่างต่อเนื่องรายปี เพื่อให้สอดคล้องกับสิ่งแวดล้อมและสถานการณ์ที่เปลี่ยนไปในแต่ละปี และนำเสนอคณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่อพิจารณาอนุมัติ - เป็นประธานในการประเมินและควบคุมความเสี่ยงและทบทวนผลการตรวจสอบประเมินความเสี่ยง รายการความเสี่ยงที่คงเหลือ (Residual Risks) และ แผนการบริหารความเสี่ยง ก่อนนำเสนอคณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่อทราบและพิจารณา - มอบแนวทางในการจัดหาทรัพยากรที่จำเป็น ให้การสนับสนุนและการทบทวนที่จำเป็นแก่ IST เพื่อให้มั่นใจว่าข้อมูลและ

ตำแหน่ง	บทบาท หน้าที่ และความรับผิดชอบ
	สินทรัพย์ที่มีค่าได้ถูกปกป้องอย่างเหมาะสม - ทบทวนและอนุมัตินโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของขั้นตอน (Procedure) แนวทางปฏิบัติ (Guideline) และเอกสารต่างๆ ที่เกี่ยวข้องในการจัดทำและพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีความเหมาะสมต่อการควบคุมความเสี่ยง - เป็นประธานในการตรวจติดตามภายใน (Internal ISMS Audit) และทบทวนผลการตรวจติดตามภายใน ก่อนนำเสนอ คณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่อทราบและพิจารณา - ทบทวนเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Incidents) ให้แนวทางในการวิเคราะห์ต้นเหตุของปัญหา และติดตามการแก้ไขปัญหา
3. คณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Team: IST)	- ทำการขับเคลื่อนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้ดำเนินการอย่างถูกต้องและดำรงรักษาไว้ซึ่งระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างต่อเนื่องตามมาตรฐาน ISO/IEC 27001:2013 - ติดตามผลการดำเนินการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) แก้ไขปัญหา และจัดทำรายงานด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ (Management Reports) อย่างต่อเนื่อง และนำเสนอต่อผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) เพื่อทราบและพิจารณา - จัดทำและปรับปรุงขอบเขต แผนงานนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) คู่มือการบริหารจัดการความเสี่ยงและอื่น ๆ ที่จำเป็น ให้สอดคล้องกับสิ่งแวดล้อมและสถานะการณ์ที่เปลี่ยนไปแต่ละปี และนำเสนอผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) เพื่อพิจารณานำเสนอ คณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่ออนุมัติต่อไป

ตำแหน่ง	บทบาท หน้าที่ และความรับผิดชอบ
	- ประเมินและควบคุมความเสี่ยงและจัดทำผลการตรวจสอบประเมินความเสี่ยงรายการความเสี่ยงที่คงเหลือ (Residual Risks) และแผนการบริหารความเสี่ยง และนำเสนอผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) เพื่อพิจารณานำเสนอคณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่ออนุมัติต่อไป - จัดทำและปรับปรุงนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของขั้นตอน (Procedure) แนวทางปฏิบัติ (Guideline) และเอกสารต่าง ๆ ที่เกี่ยวข้องในการจัดทำและพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีความเหมาะสมต่อการควบคุมความเสี่ยง - ติดตามและรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (Incidents) ให้ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) ทราบอย่างต่อเนื่อง ตลอดจนแก้ไขปัญหาตามความเหมาะสม - ทำให้มั่นใจว่าเทคนิคโครงสร้างพื้นฐาน และกระบวนการควบคุมมีความเหมาะสมและสามารถนำมาใช้งานได้อย่างถูกต้องครบถ้วน - รายงานผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) และเจ้าของสินทรัพย์ เมื่อสงสัยว่ามีการละเมิดนโยบาย หรือมีภัยคุกคามซึ่งจะมีผลกระทบกับสินทรัพย์นั้น ๆ - ประเมินการนำระบบไปใช้ทั้งในด้านนโยบายจนถึงกระบวนการ Control Self-Assessment และ Internal Audit - ประสานงานร่วมกับหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องต่าง ๆ ทั้งภายในและภายนอกองค์กร เพื่อแลกเปลี่ยนองค์ความรู้และประสบการณ์ - สร้างความตระหนักและสร้างความเข้าใจข้อกำหนดต่างๆ ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากร เพื่อยกระดับวัฒนธรรมองค์กร และการเผยแพร่

ตำแหน่ง	บทบาท หน้าที่ และความรับผิดชอบ
4. เจ้าหน้าที่ควบคุมเอกสาร (Document Controller: DC)	- รับผิดชอบเกี่ยวกับกระบวนการควบคุมเอกสาร (Document Control Procedure) - รับ และลงทะเบียนคำร้องจากผู้ริเริ่มขอเปลี่ยนแปลง/แก้ไขเอกสาร - ประสานงานเพื่อสร้างเอกสารหลัก และปรับปรุงเอกสารหลักให้ทันสมัย - ประสานงานเพื่อส่งสำเนาให้ผู้ที่มีรายชื่ออยู่ในรายชื่อการแจกจ่าย ทั้งรูปแบบอิเล็กทรอนิกส์ และเอกสาร (สิ่งพิมพ์) - ควบคุมเอกสารตามมาตรฐาน ISO/IEC 27001:2013
5. ผู้ตรวจติดตามภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Internal Auditor: IA)	- จัดเตรียมแผนการตรวจติดตามภายในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) - บริการจัดการให้มีการตรวจติดตามภายใน และติดตามความก้าวหน้าในการตรวจติดตามภายใน - สรุปผลประเมินการตรวจติดตามภายใน และจัดทำรายงานสรุปผลการตรวจติดตามภายใน - นำเสนอสรุปผลการตรวจติดตามภายในให้ ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMR) พิจารณาและนำเสนอต่อคณะผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Steering Committee) เพื่อทราบต่อไป - บริหารจัดการและปรับปรุงสถานะรายงานความไม่สอดคล้องของการปฏิบัติงาน และการให้บริการจัดทำรายงานผลการตรวจติดตามภายใน

5. ความต้องการสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Requirements for ISMS)

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ต้องมีการกำหนด จัดตั้ง นำมาใช้งาน บำรุงรักษาและปรับปรุงอย่างต่อเนื่อง โดยกำหนดจากความต้องการ และจุดประสงค์ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ กระบวนการขององค์กรที่ใช้ ขนาดและโครงสร้างขององค์กร ซึ่งสามารถเปลี่ยนแปลงได้ตลอดเวลา

เนื่องจากปัจจุบันสำนักงานคณะกรรมการส่งเสริมการลงทุนได้มีการจัดทำและดำเนินการระบบคุณภาพ (ISO 9001) ดังนั้นในการจัดทำและดำเนินการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) สำนักงานฯ จะใช้แนวทางปฏิบัติในการบริหารจัดการตามระบบคุณภาพ (ISO 9001) โดยจะเพิ่มเติมคู่มือการปฏิบัติงาน (Procedure Manual) และวิธีปฏิบัติงาน (Work Instruction) เฉพาะในส่วนที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

6. บริบทขององค์กร (Context of the organization)

6.1 ความเข้าใจในองค์กรและบริบทขององค์กร (Understanding the organization and its context) องค์กรต้องกำหนดประเด็นทั้งภายในและภายนอกที่มีผลกระทบกับจุดประสงค์และความสามารถในการบรรลุถึงผลลัพธ์ตามเป้าหมายของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

6.2 ความเข้าใจในความต้องการ และความคาดหวังขององค์กรที่เกี่ยวข้อง (Understanding the needs and expectations of interested parties) องค์กรต้องกำหนด

6.2.1 องค์กรที่เกี่ยวข้อง ซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

6.2.2 ความต้องการขององค์กร ที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

หมายเหตุ ความต้องการขององค์กรที่เกี่ยวข้องอาจรวมถึงกฎหมาย กฎระเบียบ และภาระผูกพันตามสัญญา

6.3 การกำหนดขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Determining the scope of the information security management system) องค์กรต้องกำหนดขอบเขตและการจัดตั้งขอบเขตของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ โดยระบุเป็นลายลักษณ์อักษร

เมื่อกำหนดขอบเขต องค์กรจะพิจารณา

6.3.1 ประเด็นทั้งภายในและภายนอกองค์กร ซึ่งอ้างถึง 6.1

6.3.2 ความต้องการซึ่งอ้างถึง 6.2 และ

6.3.3 ความเชื่อมต่อกันและความเกี่ยวข้องระหว่างกิจกรรม ที่ดำเนินการโดยองค์กรและโดยหน่วยงานอื่น

6.4 ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) องค์กรต้องจัดตั้ง นำมาใช้งาน รักษาไว้ และพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

7. ความเป็นผู้นำ (Leadership)

7.1 ความเป็นผู้นำและความมุ่งมั่น (Leadership and commitment)

ผู้บริหารระดับสูง (เลขาธิการ) ได้ให้คำมั่นและแสดงให้เห็นถึงความเป็นผู้นำต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดย

7.1.1 รับรองว่านโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดขึ้นสอดคล้องกับทิศทางยุทธศาสตร์ขององค์กร

7.1.2 รับรองว่ามีการบูรณาการความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ในกระบวนการขององค์กร

7.1.3 รับรองว่าให้การสนับสนุนทรัพยากรที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.1.4 สื่อสารความสำคัญของประสิทธิภาพระบบบริหารความมั่นคงปลอดภัยสารสนเทศและสอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.1.5 ให้ทิศทางและสนับสนุนบุคลากรเพื่อให้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีประสิทธิภาพ

7.1.6 ส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง

7.1.7 สนับสนุนอื่นๆ ที่แสดงถึงความเป็นผู้นำตามความรับผิดชอบ

7.2 นโยบาย (Policy)

ผู้บริหารระดับสูง (เลขาธิการ) จะกำหนดนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

7.2.1 เหมาะสมกับวัตถุประสงค์ขององค์กร

7.2.2 ครอบคลุมถึงวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ หรือเตรียมกรอบสำหรับจัดตั้งวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอ้างถึง 8.1

7.2.3 ครอบคลุมถึงความมุ่งมั่นในการบรรลุถึงความต้องการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

7.2.4 ครอบคลุมถึงความมุ่งมั่นในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศจะต้อง

7.2.5 มีการจัดทำข้อมูลเป็นเอกสาร

7.2.6 มีการสื่อสารภายในองค์กร

7.2.7 มีการเผยแพร่ประชาสัมพันธ์ให้ผู้เกี่ยวข้อง ตามความเหมาะสม

7.3 บทบาทหน้าที่ ความรับผิดชอบและการมอบอำนาจ (Organizational roles, responsibilities and authorities) ผู้บริหารระดับสูงจะต้องมั่นใจว่าความรับผิดชอบและอำนาจหน้าที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศได้ถูกมอบหมายและสื่อสารอย่างครบถ้วน ผู้บริหารระดับสูงจะต้องมองหมายความรับผิดชอบและอำนาจหน้าที่โดย

7.3.1 ต้องมั่นใจว่าระบบบริหารความมั่นคงปลอดภัยสารสนเทศสอดคล้องกับความต้องการตามมาตรฐาน ISO/IEC 27001

7.3.2 มีการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศต่อผู้บริหารระดับสูง

<u>หมายเหตุ</u> ผู้บริหารระดับสูงอาจมอบหมายความรับผิดชอบและอำนาจหน้าที่ในการรายงานประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ให้บุคลากรภายในองค์กร

8. การวางแผน (Planning)

8.1 ขั้นตอนในการระบุความเสี่ยงและโอกาส (Actions to address risks and opportunities)

8.1.1 บททั่วไป

เมื่อวางแผนสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ องค์กรจะต้องพิจารณาประเด็นที่อ้างถึงใน 6.1 และความต้องการที่อ้างถึงใน 6.2 และกำหนดความเสี่ยงและโอกาสที่ต้องจัดการเพื่อ

8.1.1.1 ให้มั่นใจว่าระบบบริหารความมั่นคงปลอดภัยสารสนเทศสามารถบรรลุเป้าหมายตามที่ตั้งไว้

8.1.1.2 ป้องกันหรือลดผลกระทบที่ไม่ปรารถนา

8.1.1.3 บรรลุผลของการปรับปรุงอย่างต่อเนื่อง

องค์กรจะต้องวางแผนดังนี้

8.1.1.4 ขั้นตอนการจัดการความเสี่ยงและโอกาส

8.1.1.5 วิธีการ

1) บูรณาการและการนำกระบวนการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศมาใช้งาน

2) ประเมินความมีประสิทธิผลของการดำเนินการ

8.1.2 การระบุความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ

องค์กรมีการกำหนดและประยุกต์ใช้กระบวนการจัดการความเสี่ยง

8.1.2.1 จัดตั้งและบำรุงรักษาเกณฑ์การประเมินความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึง

1) เกณฑ์การยอมรับความเสี่ยง

2) เกณฑ์สำหรับการประเมินความเสี่ยง

8.1.2.2 เพื่อให้มั่นใจว่ากระบวนการประเมินความเสี่ยงสามารถทำซ้ำได้ โดยได้ผลลัพธ์แบบเดิม และผลลัพธ์สามารถเปรียบเทียบได้

8.1.2.3 การระบุความเสี่ยงของการรักษาความมั่นคงปลอดภัยสารสนเทศ

1) ประยุกต์ใช้กระบวนการประเมินความเสี่ยง เพื่อระบุความเสี่ยงที่เกี่ยวกับการทำให้สูญเสียความลับ (Confidential) ความถูกต้องสมบูรณ์ (Integrity) และ ความพร้อมใช้ (Availability)

2) ระบุเจ้าของความเสี่ยง

8.1.2.4 การวิเคราะห์ความเสี่ยงของความปลอดภัยข้อมูล

1) ประเมินความเป็นไปได้ของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงที่ระบุไว้ใน 8.1.2.3 1) และ

2) ประเมินความเป็นไปได้ที่เป็นจริงของการเกิดความเสี่ยงที่ระบุใน 8.1.2.3 1)

8.1.2.5 ประเมินความเสี่ยงของความปลอดภัยข้อมูล

1) เปรียบเทียบผลของการวิเคราะห์ความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงที่กำหนดไว้ใน 8.1.2.1

2) จัดลำดับความเสี่ยงที่วิเคราะห์เพื่อจัดการความเสี่ยง

องค์กรมีการเก็บรักษาเอกสารข้อมูลเกี่ยวกับกระบวนการประเมินความเสี่ยงของความมั่นคงปลอดภัยสารสนเทศ

8.1.3 การจัดการความเสี่ยง

องค์กรมีการกำหนดและประยุกต์ใช้กระบวนการจัดการความเสี่ยง

8.1.3.1 เลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมตามผลของการประเมินความเสี่ยง

8.1.3.2 กำหนดมาตรการทั้งหมดที่จำเป็นในการนำแนวทางในการจัดการความเสี่ยงมาใช้

8.1.3.3 เปรียบเทียบมาตรการที่ระบุใน 8.1.3.2 กับมาตรการของมาตรฐาน Annex A และตรวจสอบว่าไม่มีมาตรการที่จำเป็นถูกละเว้น

8.1.3.4 จัดทำคำประกาศการนำไปใช้งาน (Statement of Applicability - SOA) ซึ่งประกอบด้วยมาตรการที่จำเป็น (ตามที่ระบุใน 8.1.3.2 และ 8.1.3.3) และการให้เหตุผลสำหรับมาตรการที่ใช้และมาตรการที่ละเว้นจาก Annex A

8.1.3.5 กำหนดแผนการจัดการความเสี่ยงของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

8.1.3.6 กำหนดเจ้าของความเสี่ยงและอนุมัติแผนการจัดการความเสี่ยง และยอมรับความเสี่ยงที่ยังคงหลงเหลือ

องค์กรมีการเก็บรักษาข้อมูลเอกสารหลักฐานเกี่ยวกับขั้นตอนการจัดการความเสี่ยงของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ทั้งนี้ในการบริหารความเสี่ยงของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) จะเป็นไปตาม แนวทางการประเมินความเสี่ยงสารสนเทศ (Risk Assessment Approach) ในวิธีปฏิบัติงาน (Work Instruction) เรื่องแนวทางการประเมินความเสี่ยงสารสนเทศ (Risk Assessment Approach) (W IT AM 02)

8.2 วัตถุประสงค์และการวางแผน เพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security objectives and planning to achieve them) องค์กรจะจัดตั้งวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในฟังก์ชั่นและระดับที่เกี่ยวข้อง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศจะต้อง

- สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- สามารถวัดผลได้ (หากปฏิบัติได้)
- คำนึงถึงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และผลจากการประเมินความเสี่ยงและการจัดการความเสี่ยง
- มีการสื่อสารกับผู้ที่เกี่ยวข้อง
- มีการปรับปรุงตามความเหมาะสม

องค์กรมีการเก็บรักษาข้อมูลเอกสารหลักฐานเกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

9. การสนับสนุน (Support)

9.1 ทรัพยากร (Resources)

องค์กรมีการระบุและเตรียมทรัพยากรที่จำเป็นในการจัดตั้งระบบบริหารความมั่นคงปลอดภัย นำมาใช้งาน บำรุงรักษา และพัฒนาอย่างต่อเนื่อง

9.2 ความสามารถ (Competence)

องค์กรดำเนินการดังนี้

9.2.1 ระบุความสามารถของบุคลากรที่จำเป็นในการปฏิบัติงานภายใต้มาตรการที่มีผลกับประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9.2.2 ทำให้มั่นใจว่าบุคลากรมีความสามารถพื้นฐานที่เหมาะสมด้านการศึกษา การฝึกอบรม และประสบการณ์

9.2.3 ดำเนินการให้ได้รับความสามารถที่จำเป็นในการปฏิบัติงาน และประเมินผลประสิทธิภาพของการดำเนินการตามความเหมาะสม

9.2.4 เก็บรักษาเอกสารหลักฐานของความสามารถนั้นๆ

<u>หมายเหตุ</u> ตัวอย่างการดำเนินการที่เหมาะสม เช่นวางแผนการฝึกอบรม การให้คำปรึกษา หรือมอบหมายงานให้บุคลากรที่มีอยู่ หรือว่าจ้างผู้ที่มีความสามารถนั้นๆ

การบริหารทรัพยากรบุคคลในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) จะเป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่องงานฝึกอบรม (P DE TR 01) และวิธีปฏิบัติงาน (Work Instruction) เรื่องแนวทางการบริหารจัดการทรัพยากรบุคคลด้านความมั่นคงปลอดภัยสารสนเทศ (Human resources security guideline) (W IT HR 01)

9.3 ความตระหนัก (Awareness)

บุคลากรที่ปฏิบัติงานภายใต้มาตการขององค์กรจะต้องตระหนักถึง

9.3.1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

9.3.2 บุคลากรให้การสนับสนุนเพื่อให้ระบบบริหารความมั่นคงปลอดภัยมีประสิทธิภาพ รวมถึงประโยชน์ที่จะได้รับเมื่อสามารถปรับปรุงประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศได้

9.3.3 การดำเนินการที่ไม่สอดคล้องกับความต้องการของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9.4 การติดต่อสื่อสาร (Communication)

องค์กรระบุความจำเป็นของทั้งการสื่อสารภายในและภายนอก ที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นไปตามวิธีปฏิบัติงาน (Work Instruction) เรื่องการสื่อสารขององค์กร (W SG IN 01) โดยคลอบคลุมสิ่งต่อไปนี้

9.4.1 สิ่งที่จะสื่อสาร

9.4.2 เวลาที่จะสื่อสาร

9.4.3 ผู้ที่จะสื่อสาร

9.4.4 ผู้ที่รับหน้าที่ผู้สื่อสาร

9.4.5 กระบวนการ ของการสื่อสารที่มีประสิทธิภาพ

9.5 เอกสารหลักฐาน (Documented information)

9.5.1 บททั่วไป

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร จะครอบคลุมถึง

9.5.1.1 ข้อมูลเอกสารที่ต้องการตามมาตรฐาน ISO/IEC 27001

9.5.1.2 ข้อมูลเอกสารที่ระบุโดยองค์กรว่ามีความจำเป็นต่อประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9.5.2 การจัดทำและปรับปรุง

เมื่อมีการจัดทำและปรับปรุงข้อมูลเอกสาร องค์กรจะต้องมั่นใจว่า

9.5.2.1 มีการระบุและคำอธิบาย (เช่น หัวเรื่อง วันที่ ผู้จัดทำ หรือหมายเลขอ้างอิง)

9.5.2.2 จัดรูปแบบ (เช่น ภาษา ซอฟต์แวร์เวอร์ชั่น กราฟฟิก) และสื่อ เช่น กระดาษ อิเล็กทรอนิกส์)

9.5.2.3 มีการทบทวนและอนุมัติตามเหมาะสม

9.5.3 การควบคุมเอกสาร

ข้อมูลเอกสารที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศมีการควบคุมเพื่อให้มั่นใจว่า

9.5.3.1 พร้อมใช้และเหมาะสมสำหรับการใช้งานในสถานที่ และเมื่อจำเป็น

9.5.3.2 มีการป้องกันอย่างพอเพียง (เช่น จากการเปิดเผยความลับ การใช้งานอย่างไม่เหมาะสม หรือขาดความสมบูรณ์)

ในการควบคุมเอกสาร องค์กรจะระบุกิจกรรมดังต่อไปนี้

9.5.3.3 การแจกจ่าย การเข้าถึง การแก้ไข และการใช้งาน

9.5.3.4 การจัดเก็บและการป้องกัน รวมถึงการดำรงไว้ซึ่งความชัดเจน

9.5.3.5 การควบคุมการเปลี่ยนแปลง (เช่น การควบคุมเวอร์ชั่น)

9.5.3.6 การเก็บรักษาและการทำลาย

เอกสารที่มาจากภายนอก มีการกำหนดตามความจำเป็นสำหรับการวางแผนและการปฏิบัติงานสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะต้องมีการระบุและควบคุมตามความเหมาะสม

การเข้าถึงหมายถึงการตัดสินใจในการให้สิทธิ์ในการดูเอกสารเท่านั้น หรือการให้สิทธิ์และอำนาจในการดูแลแก้ไขเอกสาร

เอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) รวมถึง แบบฟอร์ม และรูปแบบการบันทึกข้อมูลต่างๆ จะต้องมีการป้องกัน ควบคุม บำรุงรักษา และจัดการเอกสารให้เป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่องการควบคุมเอกสาร (P SG DC 01) และวิธีปฏิบัติงาน (Work Instruction) เรื่องการควบคุมเอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (W IT DC 01)

10. การดำเนินการ (Operation)

10.1 การวางแผนและควบคุมการดำเนินการ (Operational planning and control)

องค์กรจะต้องวางแผน จัดทำ และควบคุมกระบวนการที่จำเป็น เพื่อให้เป็นไปตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศและปฏิบัติตามข้อ 8.1 องค์กรจะต้องมีแผนการจัดทำเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดในข้อ 8.2

องค์กรจะเก็บเอกสารข้อมูลให้เป็นความตามขอบเขตที่จำเป็นเพื่อให้กระบวนการต่างๆ เป็นไปตามแผนงานที่วางไว้

หน่วยงานจะต้องควบคุมการปรับแผนและทบทวนผลของการเปลี่ยนแปลงที่ไม่ได้เจตนา เพื่อจัดการผลกระทบที่อาจจะเกิดขึ้น ตามความจำเป็น

องค์กรต้องมั่นใจว่ากระบวนการจ้างหน่วยงานอื่นดำเนินการจะมีการกำหนดและควบคุม

10.2 การประเมินความเสี่ยง (Information security risk assessment)

องค์กรจะต้องจัดทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามที่ได้วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือเกิดขึ้นโดยคำนึงถึงเกณฑ์ที่กำหนดไว้ในข้อ 8.1.2.1

องค์กรจะต้องเก็บรักษาเอกสารข้อมูลของผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

10.3 การจัดการความเสี่ยง (Information security risk treatment)

องค์กรจะต้องนำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมาใช้งาน องค์กรจะต้องเก็บรักษาเอกสารข้อมูลของผลการจัดการความเสี่ยงด้านความมั่นคงปลอดภัย

11. การประเมินผลการดำเนินการ (Performance evaluation)

11.1 การเฝ้าระวัง การวัดผล การวิเคราะห์และประเมินผล (Monitoring, measurement, analysis and evaluation) องค์กรจะต้องประเมินผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศและประสิทธิภาพของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

องค์กรจะต้องกำหนด

11.1.1 ความจำเป็นในการเฝ้าระวัง และวัดผล รวมถึงกระบวนการและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.2 วิธีการเฝ้าระวัง วัดผล วิเคราะห์ และประเมิน ตามความเหมาะสม เพื่อให้ได้ผลที่ถูกต้อง

<u>หมายเหตุ</u> วิธีการที่เลือกจะต้องสามารถเปรียบเทียบผลลัพธ์ได้ และทำซ้ำได้ผลลัพธ์ที่ถูกต้อง

11.1.3 ช่วงเวลาในการเฝ้าระวังและวัดผล

11.1.4 ผู้เฝ้าระวังและวัดผล

11.1.5 ผลที่ได้จากการเฝ้าระวังและวัดผลแล้ว จะต้องมีการวิเคราะห์และประเมินผล

11.1.6 ผู้ที่วิเคราะห์และประเมินผล

องค์กรจะเก็บรักษาเอกสารข้อมูลการเฝ้าระวังและวัดผลไว้เป็นหลักฐาน

11.2 การตรวจสอบภายใน (Internal audit)

องค์กรจะดำเนินการตรวจติดตามภายในตามรอบระยะเวลาที่กำหนดไว้ เพื่อเตรียมข้อมูลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดังนี้

11.2.1 เพื่อให้สอดคล้องกับ

- ความต้องการด้านระบบบริหารความมั่นคงปลอดภัยสารสนเทศขององค์กร
- ข้อกำหนดในมาตรฐาน ISO/IEC 27001

11.2.2 มีการนำมาใช้งานและบำรุงรักษาอย่างมีประสิทธิภาพ

11.2.3 มีการวางแผน จัดตั้ง นำมาใช้งานและบำรุงรักษาแผนการตรวจติดตาม รวมถึงความถี่ วิธีการ ความรับผิดชอบ ความต้องการของแผนและการรายงาน แผนการตรวจติดตามที่จะพิจารณาถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลจากการตรวจติดตามครั้งก่อน

11.2.4 กำหนดเกณฑ์และขอบเขตการตรวจติดตาม

11.2.5 เลือกผู้ตรวจติดตามและตรวจติดตามเพื่อให้มั่นใจว่าเป็นไปตามวัตถุประสงค์และความยุติธรรมของกระบวนการตรวจติดตาม

11.2.6 ทำให้มั่นใจว่าผลของการตรวจติดตามได้รับการรายงานต่อผู้บริหารที่เกี่ยวข้อง

11.2.7 การเก็บรักษาข้อมูลเอกสารแผนการตรวจติดตามและผลการตรวจติดตามไว้เป็นหลักฐาน

ขั้นตอนการปฏิบัติของการตรวจประเมินภายในจะเป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่อง การตรวจติดตามระบบคุณภาพภายในสำนักงาน (Internal audit) (P SG IA 01)

11.3 การทบทวนของฝ่ายบริหาร (Management review)

ผู้บริหารระดับสูงต้องทบทวนระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิผล การทบทวนของฝ่ายบริหารจะต้องพิจารณาดังนี้

11.3.1 สถานะของการดำเนินการทบทวนของฝ่ายบริหารครั้งก่อน

11.3.2 การเปลี่ยนแปลงทั้งภายในและภายนอกที่เกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

11.3.3 ข้อเสอนแนะเพื่อดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศรวมถึงแนวโน้มดังต่อไปนี้

- การไม่เป็นไปตามข้อกำหนด (Nonconformities) และการแก้ไข (Corrective Action)
- ผลการเฝ้าระวังและวัดผล
- ผลการตรวจติดตาม
- การบรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ

11.3.4 ข้อเสนอแนะจากผู้ที่เกี่ยวข้อง

11.3.5 ผลจากการประเมินความเสี่ยงและสถานะของแผนการจัดการความเสี่ยง

11.3.6 โอกาสในการพัฒนาอย่างต่อเนื่อง

ผลลัพธ์ของการทบทวนของฝ่ายบริหารจะรวมถึงการตัดสินใจที่เกี่ยวข้องกับโอกาสในการพัฒนาอย่างต่อเนื่องและความจำเป็นในการเปลี่ยนแปลงระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

องค์กรจะเก็บรักษาเอกสารข้อมูลการทบทวนของฝ่ายบริหารไว้เป็นหลักฐาน

การทบทวนโดยฝ่ายบริหารจะเป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่องการประเมินผลของระบบคุณภาพ (P SG MV 01) และวิธีปฏิบัติงาน (Work Instruction) เรื่องการประเมินผลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (W IT MV 01)

12. การปฏิบัติการแก้ไข (Improvement)

12.1 ความไม่สอดคล้องกับข้อกำหนดและการปฏิบัติการแก้ไข (Nonconformity and corrective action)

เมื่อเกิดความไม่สอดคล้องกับข้อกำหนด องค์กรจะต้อง

12.1.1 ดำเนินการกับความไม่สอดคล้องกับข้อกำหนดอย่างเหมาะสม

- ดำเนินการเพื่อควบคุมและแก้ไข
- ดำเนินการกับผลลัพธ์

12.1.2 ประเมินการดำเนินการกำจัดสาเหตุของความไม่สอดคล้องกับข้อกำหนดเพื่อไม่ให้เกิดซ้ำหรือเกิดที่อื่นอีก

- ทบทวนความไม่สอดคล้อง
- ระบุสาเหตุของความไม่สอดคล้อง
- ระบุหากเกิดความไม่สอดคล้องคล้ายกับที่เคยเกิดขึ้นหรืออาจจะเกิดขึ้นได้

12.1.3 ดำเนินการตามความจำเป็น

12.1.4 ทบทวนประสิทธิผลของการแก้ไข

12.1.5 ปรับเปลี่ยนระบบบริหารความมั่นคงปลอดภัย หากจำเป็น

การปฏิบัติการแก้ไขจะต้องเหมาะสมกับผลของความไม่สอดคล้องที่พบ โดยองค์กรจะเก็บรักษาเอกสารข้อมูลดังต่อไปนี้ไว้เป็นหลักฐาน

12.1.6 ลักษณะของความไม่สอดคล้องและการดำเนินการในภายหลัง

12.1.7 ผลการของปฏิบัติการแก้ไข

ขั้นตอนปฏิบัติสำหรับการดำเนินการเชิงแก้ไขจะเป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่อง การตรวจติดตามระบบคุณภาพภายในสำนักงาน (Internal audit) (P SG IA 01) และขั้นตอนปฏิบัติสำหรับการดำเนินการเชิงป้องกันจะเป็นไปตามคู่มือการปฏิบัติงาน (Procedure Manual) เรื่อง การปฏิบัติการป้องกัน (P SG CP 01)

12.2 การปรับปรุงอย่างต่อเนื่อง (Continual improvement)

องค์กรจะต้องคงไว้ซึ่งการปรับปรุงอย่างต่อเนื่อง เพื่อความเหมาะสมพอเพียงและสัมฤทธิผลของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ