สำหรับผู้ประกอบธุรกิจขนาดกลางและขนาดย่อม (SME)

แบบประเมินตนเองด้านการรักษาความมั่นคงปลอดภัยสารสนเทศภายใน

5 นาที

คุณก้าวทันกระแสแล้วหรือยัง?

การเปลี่ยนแปลงของภัยคุกคามและการโจมตี

- มัลแวร์เรียกค่าไถ่
- การโจมตีรหัสผ่าน
- การโจมตีทางอีเมลแบบมุ่งเป้าหมาย

การเปลี่ยนแปลงในโครงสร้างพื้นฐานด้านไอที

- คลาวด์
- แท็บเล็ต
- สมาร์ตโฟน

ใช้ **"แบบประเมินตนเองภายใน 5 นาที"** เพื่อ
ตรวจสอบสถานะความมั่นคงปลอดภัยสารสนเทศขององค์กร
ก่อนที่คุณจะสูญเสียข้อมูลไป!

ASEAN · JAPAN
Cybersecurity Cooperation

แบบประเมินตนเอง

1 โปรดอ่านคู่มือนี้ก่อนลงมือทำ

วิธีการใช้

เราให้ความสำคัญกับมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ 25 ข้อ ที่มีประสิทธิภาพและองค์กรสามารถนำไปปรับใช้ได้โดยมีต้นทุนที่ต่ำ โปรดตรวจสอบสถานะการปรับใช้มาตรการเหล่านี้และดำเนินการปรับใช้มาตรการที่องค์กรยังไม่มี โดยอ้างอิงจากคำอธิบายในแผ่นพับนี้

จุดประสงค์และข้อดี

- ช่วยให้คุณเข้าใจปัญหาขององค์กร
- เมื่อเข้าใจปัญหา คุณจะสามารถเลือกวิธีจัดการที่เฉพาะเจาะจงเพื่อดำเนินการในขั้นตอนต่อไปได้

วิธีอ่านคำอธิบาย

โปรดพิจารณาโดยไม่ต้องคำนึงถึงตัวอย่างที่ระบุในคำอธิบาย ตัวอย่างเช่น คำถามข้อที่ 16 เกี่ยวกับ "มาตรการป้องกันการโจรกรรม" ถามว่าคุณดำเนินการป้องกันการโจรกรรมโดยการเก็บแล็ปท็อปไว้ในลิ้นชักหรือไม่ และยังถามด้วยว่าในกรณีที่องค์กรของคุณไม่ใช้แล็ปท็อป คุณได้ดำเนินการป้องกันการโจรกรรมโดยการไม่ทิ้งอุปกรณ์เสริม เช่น แฟลชไดรฟ์หรือฮาร์ดไดรฟ์ภายนอก ไว้บนโต๊ะทำงานหรือไม่ โปรดใช้แผ่นพับสำหรับการอ้างอิง หากคุณไม่เข้าใจจุดประสงค์ของคำถามหรือรู้สึกว่าคำถามเข้าใจได้ยาก

หากองค์กรของคุณไม่ใช้อุปกรณ์อิเล็กทรอนิกส์ใด ๆ

รายการด้านล่างนี้อาจไม่ใช่สิ่งที่องค์กรของคุณต้องปรับใช้ ทั้งนี้ขึ้นอยู่กับประเภทของธุรกิจของคุณด้วย ในกรณีดังกล่าว ให้วงกลม "ปรับใช้แล้ว"

- ข้อที่ 4 เครื่องถ่ายเอกสารและฮาร์ดไดรฟ์ที่เชื่อมต่อกับเครือข่าย
- ข้อที่ 5 เว็บเซอร์วิส
- ข้อที่ 9 ระบบเครือข่ายไร้สาย
- ข้อที่ 23 บริการคลาวด์

หากคุณคิดว่า องค์กรของเราไม่มี 'ข้อมูลลับ'
โปรดทราบว่ารายการด้านล่างนี้คือข้อมูลลับ!

- ที่อยู่พนักงาน และสลิปเงินเดือน
- รายการค่าใช้จ่ายสำหรับพันธมิตรทางธุรกิจและข้อมูลการทำธุรกรรม
- ข้อมูลบัญชีขององค์กร
- รายชื่อลูกค้าและพันธมิตรทางธุรกิจ
- ข้อมูลการพัฒนา เช่น แบบร่างสำหรับผลิตภัณฑ์ใหม่
- ข้อมูลจากพันธมิตรทางธุรกิจที่ควรได้รับการดูแลรักษาเป็นอย่างดี

ท่ามกลางข้อมูลพื้นฐานขององค์กรจะมีข้อมูลที่ต้องรักษาไว้เป็นความลับอยู่ด้วย คุณจำเป็นต้องยืนยันและจำแนกว่าข้อมูลประเภทใดที่จัดเป็นข้อมูลลับในองค์กรของคุณ การจัดหมวดหมู่ข้อมูลเป็นขั้นตอนแรกของการรักษาความมั่นคงปลอดภัยสารสนเทศ

2 โปรดตอบคำถามทั้ง 25 ข้อในแบบประเมินตนเอง

หากคุณได้คะแนนเต็ม 100	มาตรการรักษาความมั่นคงปลอดภัยเบื้องต้นของคุณสมบูรณ์แบบอยู่แล้ว ลองพิจารณายกระดับมาตรการรักษาความมั่นคงปลอดภัยให้สูงขึ้นอีก
หากคุณได้คะแนน 70-99	การรักษาความมั่นคงปลอดภัยเกือบสมบูรณ์แบบแล้ว แต่ยังมีบางด้านที่มีมาตรการไม่สมบูรณ์
หากคุณได้คะแนน 50-69	มีมาตรการไม่เพียงพอในบางด้าน
หากคุณได้คะแนน 49 หรือน้อยกว่า	ไม่ใช่เรื่องที่น่าแปลกใจเลยหากเกิดเหตุการณ์ที่ไม่คาดคิดขึ้น เช่น ข้อมูลรั่วไหล

มาตรการที่ระบุอยู่ในแบบประเมินตนเองมีแนวคิดดังนี้

■ ผู้บริหาร (หรือผู้แทน) สามารถชี้แนะและตรวจสอบการปรับใช้มาตรการตามนโยบายได้โดยตรง
■ พนักงานทุกคนรู้จักกัน
■ องค์กรไม่มีอุปกรณ์เซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายซึ่งจำเป็นต้องมีการตั้งค่าที่ซับซ้อน

- เว็บไซต์ขององค์กรไม่ใช้เซิร์ฟเวอร์ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง เช่น การใช้บริการคลาวด์
- ไม่มีซอฟต์แวร์ที่พัฒนาขึ้นเอง และใช้ซอฟต์แวร์เชิงพาณิชย์ที่วางจำหน่ายเท่านั้น
- อนุญาตให้ใช้คอมพิวเตอร์ส่วนบุคคลในการทำงานได้ ต่อเมื่อมีการปรับใช้มาตรการแบบเดียวกับคอมพิวเตอร์ขององค์กรเท่านั้น

แบบประเมินตนเอง

แบบประเมินตนเองภายใน 5 นาที

แบบประเมินตนเองเพื่อการระบุมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศที่องค์กรของคุณควรให้ความสำคัญ

- โปรดอ่านข้อที่ 1 ในหน้าที่แล้วก่อนทำแบบประเมินนี้
- อ่านรายการประเมินด้านล่างและวงกลมในคอลัมน์ที่เหมาะสม
- แบบประเมินนี้ควรให้ผู้บริหารหรือผู้จัดการเป็นผู้กรอก
- โปรดตอบว่าพนักงานทุกคนได้ปรับใช้รายการที่มีเครื่องหมาย หรือไม่ หากมีพนักงานเพียงบางคนที่นำไปปรับใช้ ให้เลือก "ปรับใช้บางส่วน"
  โปรดตอบว่าองค์กรได้ปรับใช้รายการที่มีเครื่องหมาย หรือไม่
- ใส่คะแนนของคุณที่ด้านล่างของหน้านี้ และไปกลับอ่านข้อที่ 2 ในหน้าที่แล้ว

องค์กร

ผู้ตอบ

วันที่

รายการประเมิน	ข้อ	คำอธิบาย	คำตอบ			
			ปรับใช้แล้ว	ปรับใช้บางส่วน	ยังไม่ได้ปรับใช้	ไม่ทราบ
ส่วนที่ 1 มาตรการขั้นพื้นฐาน	1	คุณรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์โดยการอัปเดตวินโดวส์ (Windows Update)*1 อย่างสม่ำเสมอ หรือด้วยมาตรการอื่น ๆ หรือไม่	4	2	0	0
	2	คุณมีมาตรการเพื่อปกป้องคอมพิวเตอร์ของคุณจากไวรัส เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัสและอัปเดตฐานข้อมูลไวรัสอัตโนมัติหรือไม่*2	4	2	0	0
	3	คุณตั้งรหัสผ่านซึ่งเดาได้ยากและไม่ตั้งรหัสผ่านด้วยชื่อ หมายเลขโทรศัพท์ หรือวันเกิดของคุณ รวมถึงหลีกเลี่ยงการใช้รหัสผ่านซ้ำกันในเว็บเซอร์วิสต่าง ๆ หรือไม่	4	2	0	0
	4	คุณจำกัดการเข้าถึงข้อมูลสำคัญอย่างเหมาะสม เช่น จำกัดสิทธิในการใช้งานเครื่องถ่ายเอกสารหรือฮาร์ดไดรฟ์ที่เชื่อมต่อเครือข่าย โดยสงวนสิทธิ์การเข้าถึงแก่ผู้ที่จำเป็นต้องใช้งานเท่านั้น หรือไม่	4	2	0	0
	5	คุณเตรียมระบบไว้สำหรับระบุภัยคุกคามและการโจมตีรูปแบบใหม่ ๆ และมีการตรวจสอบและแชร์การแจ้งเตือนด้านการรักษาความมั่นคงปลอดภัยจากเจ้าของผลิตภัณฑ์หรือเว็บเซอร์วิส*3 ที่คุณใช้อยู่หรือไม่	4	2	0	0
ส่วนที่ 2 มาตรการในฐานะพนักงาน	6	คุณมีความตระหนักต่ออีเมลฟิชชิ่ง และไม่เปิดไฟล์แนบหรือคลิกลิงก์ในอีเมลที่น่าสงสัยหรือไม่	4	2	0	0
	7	คุณเตรียมระบบสำหรับตรวจสอบและป้องกันการส่งอีเมลผิดพลาด เช่น การตรวจดูที่อยู่อีเมลก่อนส่งหรือไม่	4	2	0	0
	8	คุณปกป้องข้อมูลสำคัญโดยการเข้ารหัสลับไฟล์แนบหรือใช้มาตรการที่ใกล้เคียงกันก่อนส่งอีเมลหรือไม่	4	2	0	0
	9	คุณดำเนินการรักษาความมั่นคงปลอดภัยเครือข่ายไร้สาย เช่น เข้ารหัสลับด้วยวิธีการมั่นคงปลอดภัยอย่างสม่ำเสมอ หรือไม่	4	2	0	0
	10	คุณควบคุมการใช้งานอินเทอร์เน็ต เช่น ตั้งกฎการใช้งานเว็บเบราว์เซอร์และการโพสต์บนโซเชียลมีเดียด้วยคอมพิวเตอร์ขององค์กร หรือไม่	4	2	0	0
	11	คุณดำเนินการสำรองข้อมูลอย่างสม่ำเสมอเพื่อป้องกันข้อมูลสำคัญสูญหายในกรณีที่เกิดความผิดปกติหรือข้อผิดพลาด หรือไม่	4	2	0	0
	12	คุณดำเนินการป้องกันการสูญเสียหรือการรั่วไหลของข้อมูลสำคัญ เช่น การจัดเก็บข้อมูลสำคัญไว้ในตู้เก็บเอกสารแทนการวางไว้บนโต๊ะทำงาน หรือไม่	4	2	0	0
	13	หากคุณจำเป็นต้องนำข้อมูลสำคัญออกไปภายนอกสำนักงาน คุณมีการดำเนินการป้องกันการโจรกรรมหรือการสูญหาย เช่น ป้องกันด้วยการใช้รหัสผ่านหรือการเข้ารหัสลับและเก็บข้อมูลนั้นไว้กับตัวเองตลอดเวลา หรือไม่	4	2	0	0
	14	คุณดำเนินการให้แน่ใจว่าจะไม่มีผู้อื่นมาใช้งานคอมพิวเตอร์ของคุณได้ เช่น ตั้งค่าล็อคหน้าจอคอมพิวเตอร์เวลาที่คุณลุกออกจากโต๊ะทำงาน หรือไม่	4	2	0	0
	15	เมื่อคุณพบเห็นบุคคลที่ไม่คุ้นหน้าในสำนักงาน คุณพยายามเข้าไปห้ามหรือใช้มาตรการอื่น ๆ เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่สำนักงาน หรือไม่	4	2	0	0
	16	คุณป้องกันการโจรกรรมเมื่อคุณออกจากสำนักงาน เช่น การเก็บแล็ปท็อปและอุปกรณ์เสริมอื่น ๆ ในลิ้นชักแทนการวางไว้บนโต๊ะทำงาน หรือไม่	4	2	0	0
	17	กุญแจสำนักงานได้รับการดูแลอย่างเหมาะสม เช่น ให้ผู้ที่ออกจากสำนักงานคนสุดท้ายล็อคสำนักงานและจดบันทึก (ชื่อ วันและเวลาที่ออก) หรือไม่	4	2	0	0
	18	เมื่อต้องทำลายข้อมูลสำคัญ คุณจัดการข้อมูลสำคัญให้อยู่ในสภาพที่ไม่สามารถนำกลับมาอ่านได้อีก เช่น การใช้เครื่องทำลายเอกสารหรือเครื่องมือลบข้อมูล หรือไม่	4	2	0	0
ส่วนที่ 3 มาตรการในฐานะองค์กร	19	คุณมีหลักจรรยาบรรณสำหรับพนักงานเพื่อรักษาความลับของข้อมูล เช่น การแจ้งพนักงานว่าพวกเขามีหน้าที่รักษาความลับของข้อมูลและมีบทลงโทษหากเพิกเฉย หรือไม่	4	2	0	0
	20	คุณจัดการฝึกอบรมเกี่ยวกับความตระหนักในการรักษาความมั่นคงปลอดภัยเพื่อช่วยให้พนักงานรับรู้ถึงความสำคัญของการบริหารข้อมูลสำคัญ เช่น การอธิบายความสำคัญของการบริหารข้อมูลสำคัญอย่างสม่ำเสมอ หรือไม่	4	2	0	0
	21	คุณชี้แจงต่อพนักงานเรื่องการใช้อุปกรณ์ส่วนบุคคลในการทำงาน เช่น การตั้งนโยบายการใช้งานคอมพิวเตอร์และสมาร์ตโฟนส่วนบุคคลทั้งภายในและภายนอกองค์กร หรือไม่	4	2	0	0
	22	คุณแจ้งให้พันธมิตรทางธุรกิจรักษาความลับของข้อมูล เช่น การระบุข้อกำหนด/ข้อผูกมัดในการรักษาความลับของข้อมูลไว้ในสัญญา หรือไม่	4	2	0	0
	23	คุณยืนยันความปลอดภัยและความน่าเชื่อถือของการบริการโดยการตรวจสอบข้อตกลงในการใช้งานและมาตรการรักษาความมั่นคงปลอดภัยก่อนการเลือกใช้บริการภายนอก เช่น บริการคลาวด์ หรือไม่	4	2	0	0
	24	คุณเตรียมความพร้อมสำหรับกรณีเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น ร่างกระบวนการสำหรับตอบสนองต่อเหตุการณ์ข้อมูลลับรั่วไหล สูญหาย หรือถูกโจรกรรม หรือไม่	4	2	0	0
	25	คุณกำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น การประกาศมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (เช่น ข้อที่ 1 ถึง 24 ข้างต้น) เป็นนโยบายขององค์กร หรือไม่	4	2	0	0

A คะแนนรวมสำหรับการปรับใช้มาตรการทั้งหมด	B คะแนนรวมสำหรับการปรับใช้มาตรการบางส่วน	A+B คะแนน
คะแนน	คะแนน	คะแนน

*1 โปรแกรมของบริษัทไมโครซอฟต์ที่ช่วยแก้ข้อบกพร่องบนคอมพิวเตอร์ระบบวินโดวส์

*2 ไฟล์ฐานข้อมูลที่เรียกว่า "ไฟล์รูปแบบ" สำหรับตรวจจับไวรัสคอมพิวเตอร์

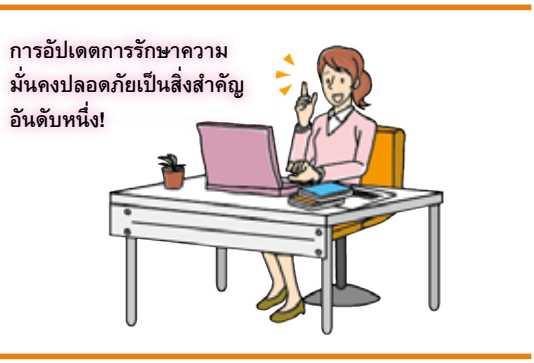
*3 ชื่อสามัญของบริการที่ใช้อินเทอร์เน็ต เช่น อินเทอร์เน็ตแบงค์กิ้ง โซเชียลมีเดีย เว็บเมล และปฏิทิน

★ ไม่สามารถรับประกันได้ว่ามาตรการตามที่อธิบายในแบบประเมินตนเองสามารถให้ความคุ้มครองได้อย่างสมบูรณ์แบบ

คำอธิบาย

ส่วนที่ 1 มาตรการขั้นพื้นฐาน

ข้อที่ 1 ถึง 5 คือมาตรการที่ควรปรับใช้ไม่ว่าองค์กรจะมีขนาดหรือรูปแบบใดก็ตาม และเป็นสิ่งสำคัญมากที่มาตรการเหล่านี้ต้องได้รับการตรวจทานอย่างต่อเนื่องและไม่ใช่เพียงครั้งเดียว องค์กรจำเป็นต้องปรับใช้มาตรการเหล่านี้เป็นกฎขององค์กร เพื่อให้พนักงานทุกคนสามารถปฏิบัติตามได้



รายการที่ 1 มาตรการจัดการช่องโหว่

หมั่นอัปเดตระบบปฏิบัติการและซอฟต์แวร์ของคุณอยู่เสมอ

การเพิกเฉยต่อปัญหาความมั่นคงปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์ของคุณ จะเพิ่มความเสี่ยงให้อุปกรณ์ของคุณติดไวรัสร้ายแรงได้ โปรดตรวจสอบให้แน่ใจว่ามีการอัปเดตแพทช์หรือใช้เวอร์ชั่นล่าสุดของระบบปฏิบัติการและซอฟต์แวร์ของคุณ

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การใช้ Windows Update (ระบบปฏิบัติการวินโดวส์) หรือใช้ Adobe Flash Player, Adobe Reader, Java Runtime Environment และซอฟต์แวร์อื่น ๆ ในเวอร์ชั่นล่าสุด

รายการที่ 2 มาตรการป้องกันไวรัส

ติดตั้งซอฟต์แวร์ป้องกันไวรัสและใช้งานอย่างเหมาะสม

ปัจจุบันมีไวรัสที่ขโมยบัญชีและรหัสผ่าน ใช้งานคอมพิวเตอร์ในระยะไกล และเข้ารหัสลับโดยพลการในปริมาณที่มากขึ้น โปรดติดตั้งซอฟต์แวร์ป้องกันไวรัสและตรวจสอบให้แน่ใจว่าฐานข้อมูลไวรัส (ไฟล์รูปแบบ) อัปเดตเป็นรุ่นปัจจุบันอยู่เสมอ

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การตั้งค่าอุปกรณ์ของคุณให้อัปเดตฐานข้อมูลไวรัสโดยอัตโนมัติและพิจารณาการติดตั้งชุดซอฟต์แวร์รักษาความมั่นคงปลอดภัย

รายการที่ 3 การบริหารจัดการรหัสผ่าน

ใช้รหัสผ่านที่ปลอดภัย

ปัจจุบันมีความเสียหายในปริมาณที่มากขึ้นที่เกิดจากการล็อกอินที่ไม่ได้รับอนุญาตอันเนื่องมาจากรหัสผ่านที่สามารถเดาได้ง่าย รวมถึงการนำบัญชีและรหัสผ่านที่รั่วไหลจากเว็บเซอร์วิสไปใช้ในทางที่ผิด โปรดตั้งรหัสผ่านที่ปลอดภัยโดยการกำหนดรหัสให้มีความยาวและซับซ้อน รวมถึงไม่นำไปใช้ซ้ำกับบัญชีอื่น

*รหัสผ่านแบบง่าย: รหัสผ่านที่บุคคลที่สามสามารถเดาได้โดยง่าย เช่น ชื่อของคุณ ชื่อองค์กร หรือคำภาษาอังกฤษง่าย ๆ ในพจนานุกรม

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การตั้งรหัสผ่านที่ประกอบด้วยตัวอักษร ตัวเลข และเครื่องหมาย 10 ตัวขึ้นไป ห้ามใช้ชื่อ หมายเลขโทรศัพท์ วันเกิด ฯลฯ รวมถึงห้ามใช้รหัสผ่านซ้ำกันกับที่ตั้งไว้ในเว็บเซอร์วิสและเว็บไซต์อื่น ๆ

รายการที่ 4 การตั้งค่าอุปกรณ์

ตรวจทานการตั้งค่าการแบ่งปัน

ปัจจุบันมีความกังวลที่มากขึ้น จากการเข้าถึงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาตอันเนื่องมาจากข้อมูลนั้นถูกจัดเก็บในไฟล์เซิร์ฟเวอร์ คลังเก็บข้อมูลออนไลน์ หรือเครื่องถ่ายเอกสารที่ตั้งค่าผิด โปรดตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์และอุปกรณ์ที่เชื่อมต่อเครือข่ายนั้นถูกตั้งค่าให้แบ่งปันเฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูลได้เท่านั้น

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การจำกัดขอบเขตการแบ่งปันบริการคลาวด์ การจำกัดขอบเขตการแบ่งปันอุปกรณ์ที่เชื่อมต่อเครือข่าย และการเปลี่ยนการตั้งค่าเมื่อพนักงานมีการโยกย้ายส่วนงานหรือถูกเลิกจ้าง

รายการที่ 5 การรวบรวมข้อมูล

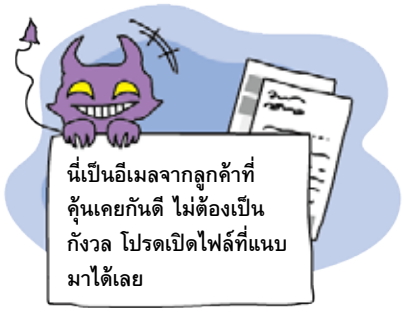
เรียนรู้เกี่ยวกับภัยคุกคามและเทคนิคการโจมตี รวมถึงขั้นตอนการรับมือ

ปัจจุบันมีการโจมตีแบบฟิชชิ่งในปริมาณที่มากขึ้น เพื่อโจรกรรมบัญชีและรหัสผ่านทางอีเมลที่แนบไฟล์ติดไวรัสโดยลวงว่าเป็นพันธมิตรทางธุรกิจหรือผู้มีส่วนได้เสีย หรือลวงด้วยการปลอมแปลงเว็บไซต์ที่เลียนแบบเว็บไซต์ถูกกฎหมาย โปรดเรียนรู้วิธีรับมือกับภัยคุกคามและการโจมตี

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การตรวจสอบเว็บไซต์ IPA และสมัครสมาชิกนิตยสารทางอีเมลเพื่อเรียนรู้เกี่ยวกับภัยคุกคามและรูปแบบการโจมตีล่าสุด รวมถึงตรวจสอบการแจ้งเตือนจากอินเทอร์เน็ตแบงค์กิ้งและบริการอื่น ๆ ที่ใช้บริการ

ส่วนที่ 2 มาตรการในฐานะพนักงาน

ข้อที่ 6 ถึง 18 เป็นมาตรการที่พนักงานควรรับรู้ไว้ ความผิดพลาดของมนุษย์สามารถเกิดขึ้นได้ง่ายเนื่องจากต้องดูแลข้อมูลสำคัญเป็นประจำจนรู้สึกคุ้นเคยเป็นอย่างดี ซึ่งอาจทำให้ผู้นั้นละเลยหน้าที่ของตัวเองได้ นอกจากนั้น รูปแบบภัยคุกคามนั้นมีการเปลี่ยนแปลงอยู่ตลอดเวลา คุณจึงจำเป็นต้องระมัดระวังอยู่เสมอ



รายการที่ 6	กฎการใช้อีเมล

ระมัดระวังอีเมลที่ส่งมาจากบุคคลที่คุณไม่รู้จัก

อีเมลแบบนี้สามารถทำให้เครื่องติดไวรัสได้เพียงแค่เปิดไฟล์ที่แนบมากับอีเมลหรือคลิกลิงก์ URL ในส่วนเนื้อหาของอีเมล โปรดระมัดระวังไฟล์ที่แนบมาและการคลิกลิงก์ URL จากผู้ส่งที่คุณไม่รู้จัก

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น ไม่เปิดไฟล์ที่แนบมาหรือคลิกลิงก์ URL ในอีเมลน่าสงสัย รวมถึงรายงานอีเมลน่าสงสัยเหล่านั้นกับฝ่ายรักษาความมั่นคงปลอดภัยเพื่อให้ข้อมูลเกี่ยวกับอีเมลน่าสงสัยในองค์กร

รายการที่ 7	กฎการใช้อีเมล

ระวังส่งอีเมลให้ผิดคน

กรณีข้อมูลรั่วไหลสามารถเกิดขึ้นได้จากการส่งอีเมลหรือแฟกซ์ถึงผู้รับผิดคน โปรดตรวจสอบให้แน่ใจว่าคุณได้ตรวจทานดีแล้วว่าคุณกำลังส่งอีเมลหรือแฟกซ์ให้ใคร นอกจากนั้น ข้อมูลก็สามารถรั่วไหลได้ในกรณีที่คุณบอกที่อยู่อีเมลผิด หากต้องส่งอีเมลให้ผู้รับหลายคน ตรวจสอบให้แน่ใจว่าที่อยู่อีเมลของผู้รับนั้นถูกต้องดีแล้ว

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การตรวจสอบซ้ำก่อนการส่งอีเมลหรือแฟกซ์ รวมถึงเลือกที่อยู่ To, CC, และ BCC ทีละช่อง

รายการที่ 8	กฎการใช้อีเมล

ป้องกันข้อมูลสำคัญเมื่อส่งอีเมล

หากต้องส่งข้อมูลสำคัญทางอีเมล ห้ามเขียนข้อมูลนั้นลงในเนื้อหาของอีเมล ให้เขียนข้อมูลในไฟล์ ใส่รหัสผ่าน และแนบไฟล์นั้นกับอีเมลแทน แจ้งรหัสผ่านแก่ผู้รับอีเมลทางโทรศัพท์หรือทางอื่นแทนการเขียนลงไปในอีเมล

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การเขียนข้อมูลสำคัญลงในไฟล์และใส่รหัสผ่านไว้ แจ้งรหัสผ่านแก่ผู้รับทางโทรศัพท์หรือทางอื่น ๆ

รายการที่ 9	กฎการใช้เครือข่ายไร้สาย

ป้องกันการดักฟังและการนำเครือข่ายไร้สายไปใช้งานโดยไม่ได้รับอนุญาต

เครือข่ายไร้สายที่ไม่มีการตั้งค่าความปลอดภัยอย่างเหมาะสมอาจถูกล้วงข้อมูลหรือนำระบบไปใช้ในเชิงอาชญากรรมด้วยการเชื่อมต่ออย่างผิดกฎหมาย ตรวจสอบให้แน่ใจว่าได้ตั้งค่าความปลอดภัยของเครือข่ายไร้สายเพื่อป้องกันการถูกดักฟังและนำไปใช้โดยไม่ได้รับอนุญาต

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การใช้การตั้งค่าเข้ารหัสลับ (เช่น WPA2-PSK) และใช้รหัสผ่านที่ยาวและเดาได้ยาก

รายการที่ 10	กฎการใช้อินเทอร์เน็ต

ป้องกันปัญหาขณะใช้อินเทอร์เน็ต

การเข้าดูเว็บไซต์หลอกลวงหรือเว็บไซต์ที่มีปัญหาด้านการรักษาความมั่นคงปลอดภัยอาจทำให้อุปกรณ์ของคุณติดไวรัสได้ นอกจากนั้น องค์กรอาจได้รับความเสียหายจากการโพสต์มุกล้อเลียนองค์กรบนโซเชียลมีเดียหรือเว็บบอร์ด หรือจากการโพสต์ข้อมูลลับโดยไม่ตั้งใจ ดังนั้นจึงจำเป็นต้องมีการป้องกันมิให้เกิดความเสียหายโดยการปรับใช้ระบบและกฎระเบียบที่จำกัดการใช้อินเทอร์เน็ตในที่ทำงาน

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การตั้งกฎการเข้าถึงสำหรับการใช้อินเทอร์เน็ตและโซเชียลมีเดีย และใช้ตัวกรองเว็บเพื่อจำกัดการใช้อินเทอร์เน็ตอย่างเป็นระบบ

รายการที่ 11	กฎการสำรองข้อมูล

หมั่นสำรองข้อมูลอย่างสม่ำเสมอ

ข้อมูลที่บันทึกอยู่บนคอมพิวเตอร์หรือเซิร์ฟเวอร์อาจสูญหายเนื่องจากความผิดปกติ ข้อผิดพลาดในการทำงาน หรือติดไวรัสได้ โปรดสำรองข้อมูลเพื่อเตรียมตัวสำหรับสถานการณ์ที่ไม่คาดคิด

การดำเนินการ ปฏิบัติตามขั้นตอน เช่น การสำรองข้อมูลสำคัญอย่างสม่ำเสมอและจัดเก็บข้อมูลสำรองในสถานที่ที่แยกไว้ต่างหาก

คำอธิบาย

รายการที่ 12 กฎการจัดเก็บข้อมูล

ข้อมูล/เอกสารสำคัญต้องได้รับการดูแลอย่างเหมาะสม

การวางข้อมูล/เอกสารไว้บนโต๊ะทำงานโดยปราศจากผู้ดูแลถือเป็นเรื่องที่อันตราย เพราะอาจมีบุคคลอื่นมานำไปอ่านได้ ข้อมูล/เอกสารสำคัญต้องได้รับการดูแลอย่างเหมาะสม ตรวจสอบให้แน่ใจว่าไม่วางข้อมูล/เอกสารสำคัญทิ้งไว้บนโต๊ะทำงาน กำหนดตำแหน่งในการจัดเก็บข้อมูล/เอกสาร นำออกมาเฉพาะช่วงที่จำเป็นต้องใช้งาน และตรวจสอบให้แน่ใจว่าได้จัดเก็บกลับเข้าที่เดิมหลังเสร็จสิ้นการใช้งาน

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การจัดโต๊ะทำงานให้สะอาดเรียบร้อย รวมถึงจัดเก็บข้อมูล/เอกสารสำคัญล็อคไว้ในตู้เก็บเอกสาร**

รายการที่ 13 กฎการเคลื่อนย้ายข้อมูล

เคลื่อนย้ายข้อมูลสำคัญอย่างปลอดภัย

เมื่อต้องนำข้อมูลสำคัญออกไปภายนอกองค์กรก็จะมีโอกาสที่ข้อมูลนั้นจะถูกโจรกรรมหรือสูญหายได้ โปรดเตรียมมาตรการรักษาความมั่นคงปลอดภัยสำหรับแล็ปท็อปหรือสมาร์ตโฟนก่อนการใช้งาน เช่น การตั้งรหัสผ่านหรือเข้ารหัสลับไฟล์ข้อมูล เพื่อให้ข้อมูลนั้นไม่สามารถถูกเปิดดูได้ง่ายในกรณีที่เกิดถูกโจรกรรมหรือสูญหาย

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การออกมาตรการให้ต้องขออนุญาตก่อนทำการเคลื่อนย้ายข้อมูลสำคัญ การรักษาความมั่นคงปลอดภัยสารสนเทศด้วยการตั้งรหัสผ่านบนแล็ปท็อป สมาร์ตโฟน หรือแฟลชไดรฟ์ รวมถึงห้ามวางสัมภาระทิ้งไว้โดยปราศจากผู้ดูแล**

รายการที่ 14 การบริหารจัดการความปลอดภัยในสำนักงาน

ห้ามให้ผู้อื่นใช้อุปกรณ์ต่าง ๆ โดยไม่ได้รับอนุญาต

ผู้อื่นสามารถใช้งานเครื่องคอมพิวเตอร์ที่ปราศจากผู้ดูแลในทางที่ผิดได้ โปรดป้องกันคอมพิวเตอร์จากการใช้งานที่ไม่ได้รับอนุญาต เช่น ไม่เปิดคอมพิวเตอร์ทิ้งไว้โดยปราศจากผู้ดูแลและตั้งรหัสผ่านบนอุปกรณ์

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การล็อคคอมพิวเตอร์เมื่อคุณไม่อยู่ที่โต๊ะทำงานของตัวเอง การปิดเครื่องคอมพิวเตอร์เมื่อคุณออกจากสำนักงาน และไม่ให้ผู้อื่นมาใช้คอมพิวเตอร์ของคุณ**

รายการที่ 15 การบริหารจัดการความปลอดภัยในสำนักงาน

เข้าพูดคุยกับบุคคลที่คุณไม่คุ้นหน้า

ข้อมูลมีความเสี่ยงต่อการถูกโจรกรรมหากคุณไม่ห้ามผู้ที่ไม่ได้รับอนุญาตมิให้เข้ามาในสำนักงาน ตรวจสอบให้แน่ใจว่ามีการห้ามผู้ที่ไม่ได้รับอนุญาตเข้าไปยังพื้นที่ที่ใช้จัดเก็บข้อมูล/เอกสารสำคัญ โดยเฉพาะเซิร์ฟเวอร์ คลังจัดเก็บข้อมูล และตู้เซฟ

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การเข้าพูดคุยกับบุคคลที่คุณไม่รู้จักในสำนักงานหรือบริการเคาน์เตอร์ต้อนรับ**

รายการที่ 16 การบริหารจัดการความปลอดภัยในสำนักงาน

ป้องกันการโจรกรรมอุปกรณ์และอุปกรณ์เสริม

อุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์แล็ปท็อป แท็บเล็ต และแฟลชไดรฟ์ นั้นสะดวกและพกพาง่าย แต่ในขณะเดียวกันก็เสี่ยงต่อการถูกโจรกรรมเช่นกัน เมื่อไม่ใช้งานให้จัดเก็บอุปกรณ์ไว้ในที่ที่ปลอดภัย เช่น ในลิ้นชักที่สามารถล็อคได้

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การล็อคแล็ปท็อป แท็บเล็ต และอุปกรณ์เสริม (แผ่นซีดี แฟลชไดรฟ์ ฮาร์ดไดรฟ์ภายนอก เป็นต้น) ในลิ้นชักโต๊ะทำงานเมื่อออกจากสำนักงาน**

รายการที่ 17 การบริหารจัดการความปลอดภัยในสำนักงาน

ระมัดระวังเรื่องการล็อคประตูสำนักงาน

การให้บุคคลที่ออกจากสำนักงานคนสุดท้ายทำการจดบันทึกเวลาออกจากสำนักงานก็สามารถช่วยให้บุคคลดังกล่าวรู้สึกว่าต้องรับผิดชอบในการล็อคประตูด้วย หมั่นดูแลรักษากุญแจและจดบันทึกอยู่เสมอ

การดำเนินการ **ปฏิบัติตามขั้นตอน เช่น การดูแลรักษากุญแจและให้บุคคลที่ออกจากสำนักงานคนสุดท้ายเป็นผู้ล็อคประตูและจดบันทึกไว้ (วันที่ เวลา และชื่อ)**

รายการที่ 18 การทำลายข้อมูลอย่างปลอดภัย

กำจัดข้อมูลสำคัญเพื่อให้ไม่สามารถนำกลับมาใช้ใหม่ได้

การทิ้งเอกสารที่มีข้อมูลสำคัญลงถังขยะอาจนำไปสู่เหตุการณ์ข้อมูลรั่วไหลที่ร้ายแรงได้ เนื่องจากเอกสารดังกล่าวยังสามารถถูกพบโดยบุคคลอื่นได้ นอกจากนั้น ข้อมูลที่บันทึกไว้บนสื่ออิเล็กทรอนิกส์ก็สามารถกู้คืนมาได้ถึงแม้จะลบข้อมูลไปแล้วก็ตาม ดังนั้น เมื่อต้องทำลายข้อมูลสำคัญ ให้ทำลายข้อมูลด้วยวิธีที่เหมาะสม เช่น การใช้เครื่องทำลายเอกสารหรือซอฟต์แวร์สำหรับลบข้อมูล

การดำเนินการ **ลงมือทำลายข้อมูล เช่น การใช้ซอฟต์แวร์ลบข้อมูล ทำลายอุปกรณ์เก็บข้อมูล หรือให้ผู้เชี่ยวชาญช่วยดำเนินการลบข้อมูล**

จัดเก็บเอกสารที่มีข้อมูลสำคัญล็อคไว้ในลิ้นชัก

ป้องกันการขโมยอุปกรณ์

ล็อคประตูสำนักงาน

ส่วนที่ 3 มาตรการในฐานะองค์กร

ข้อที่ 19 ถึง 25 เป็นมาตรการที่ต้องปรับใช้หลังจากการตั้งนโยบายสำหรับองค์กร สร้างความตระหนักแก่พนักงานโดยการจัดทำกฎการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรอย่างชัดเจนและแบ่งปันกันภายในสำนักงาน

รายการที่ 19	การแจ้งพนักงานถึงความรับผิดชอบของตนเองในการรักษาความลับ

ให้พนักงานทำความเข้าใจความรับผิดชอบของตนเองในการรักษาความลับ

ถึงแม้กฎระเบียบองค์กรจะกำหนดให้พนักงานรักษาความลับในการทำงานไว้อยู่แล้ว แต่จะได้ผลลัพธ์ที่ดีกว่าหากแจ้งกฎระเบียบองค์กรอย่างชัดเจนเพื่อให้พนักงานได้ปฏิบัติตาม

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การแจ้งพนักงานถึงความรับผิดชอบของตนเองในการรักษาความลับหลังจากการจ้างงาน

รายการที่ 20	การฝึกอบรมพนักงาน

จัดการฝึกอบรมพนักงานอย่างสม่ำเสมอ

พนักงานจะทำงานกับข้อมูลเป็นประจำทุกวัน และความคุ้นเคยนี้ก็มักจะนำไปสู่การละเลยและพวกเขาก็จะลืมว่าต้องบริหารข้อมูลด้วยความปลอดภัย การฝึกอบรมพนักงานอย่างสม่ำเสมอมีส่วนช่วยในการเพิ่มความตระหนักของพนักงาน

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การอธิบายความสำคัญของการบริหารข้อมูลและจัดการฝึกอบรมภายในองค์กรอย่างสม่ำเสมอ

รายการที่ 21	การใช้งานอุปกรณ์ส่วนบุคคล

กำหนดว่าอนุญาตให้ใช้งานอุปกรณ์ส่วนบุคคลสำหรับการทำงานได้หรือไม่

ตรวจสอบให้แน่ใจว่าการรักษาความมั่นคงปลอดภัยมีความรัดกุมมากขึ้นหากมีการใช้งานอุปกรณ์ส่วนบุคคลในการทำงาน เช่น คอมพิวเตอร์และสมาร์ตโฟน เนื่องจากการควบคุมพนักงานในกรณีนี้จะทำได้ยาก ดังนั้น ควรกำหนดว่าอนุญาตให้ใช้งานอุปกรณ์ส่วนบุคคลสำหรับการทำงานได้หรือไม่ และตั้งกฎระเบียบจำกัดการใช้งาน

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การจัดตั้งระบบขออนุญาตสำหรับการใช้งานอุปกรณ์ส่วนบุคคลในการทำงาน เช่น คอมพิวเตอร์และสมาร์ตโฟน และกำหนดกฎระเบียบสำหรับการใช้งานหากอนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนบุคคลในการทำงานได้

รายการที่ 22	การบริหารพันธมิตรทางธุรกิจ

ขอให้พันธมิตรทางธุรกิจรักษาความลับของข้อมูล

อย่าทึกทักเอาเองว่าพันธมิตรจะรักษาความลับตามประเภทของข้อมูล เมื่อส่งมอบข้อมูลลับให้แก่พันธมิตรทางธุรกิจจำเป็นต้องชี้แจงด้วยว่าให้พวกเขาเก็บข้อมูลนั้นเป็นความลับด้วย

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การร่างสัญญาที่ชี้แจงว่าให้พันธมิตรทางธุรกิจรักษาเนื้อหาเป็นความลับ

รายการที่ 23	การใช้งานบริการภายนอก

ใช้บริการภายนอกที่มีความน่าเชื่อถือ

หากคุณจะเลือกใช้บริการภายนอก เช่น บริการคลาวด์ โดยยึดเอาต้นทุนเป็นหลัก คุณอาจจะพบว่าคุณไม่สามารถใช้บริการได้เนื่องจากข้อผิดพลาดและปัญหาอื่น ๆ ให้ตรวจสอบการทำงาน ความน่าเชื่อถือ รายละเอียดการชดเชย และรายละเอียดอื่น ๆ ที่เกี่ยวข้องอย่างละเอียดเมื่อมีการใช้งานบริการภายนอกโดยเฉพาะการปรับใช้ที่มีผลกระทบอย่างมากต่อความต่อเนื่องทางธุรกิจ

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การตรวจสอบเงื่อนไขการบริการ รายละเอียดการชดเชย มาตรการรักษาความมั่นคงปลอดภัย และรายละเอียดอื่น ๆ ที่เกี่ยวข้องเมื่อทำการเลือกผู้ให้บริการ

คำอธิบาย

รายการที่ 24	การเตรียมตัวสำหรับเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

เตรียมตัวสำหรับเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศไว้ล่วงหน้า

เมื่อเกิดเหตุการณ์ขึ้น คุณมักไม่มีเวลาให้ขบคิด และความล่าช้าในการจัดการปัญหาก็มักทำให้เกิดผลกระทบมากยิ่งขึ้น อ้างอิงเหตุการณ์ที่เคยถูกนำมารายงานในสื่อมวลชนเพื่อพิจารณาว่าใครต้องทำอะไร เมื่อไหร่ อย่างไร โดยการสมมติว่าเหตุการณ์ดังกล่าวเกิดขึ้นกับองค์กรของคุณ

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การเตรียมคู่มือการแก้ปัญหาสำหรับข้อมูลสำคัญรั่วไหล สูญหาย หรือถูกโจรกรรม

รายการที่ 25	กฎการเตรียมตัว

ตั้งกฎสำหรับมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ

ถึงแม้ผู้บริหารจะตั้งนโยบายสำหรับมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศไว้แล้ว แต่พนักงานก็จำเป็นต้องปรึกษาผู้จัดการของตัวเองอยู่ตลอดเวลา ยกเว้นในกรณีที่องค์กรระบุกฎระเบียบเป็นลายลักษณ์อักษรไว้อย่างชัดเจน เพื่อให้พนักงานสามารถดำเนินการตามกฎระเบียบของตัวเองได้ "กฎระเบียบองค์กร" จำเป็นต้องได้รับการจัดทำเป็นลายลักษณ์อักษรอย่างชัดเจนสำหรับให้พนักงานใช้อ้างอิงเมื่อต้องการ

การดำเนินการ	ปฏิบัติตามขั้นตอน เช่น การนำเอาข้อที่ 1-24 ของแบบประเมินมาปรับใช้เป็นกฎระเบียบสำหรับมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและแบ่งปันกันภายในองค์กร รวมถึงตรวจทานกฎระเบียบเหล่านี้อย่างสม่ำเสมอเพื่อปรับปรุงในกรณีที่พบข้อบกพร่อง

NISC National center of Incident readiness and Strategy for Cybersecurity
ETDA สพธอ www.etda.or.th
IPA Information-technology Promotion Agency, Japan
2019.04