



ประกาศธุรกิจอุปการณ์การเกษตร

ที่ ธอก. 028/2566

เรื่อง นโยบายและแนวปฏิบัติระดับเครือ : การจัดหาอย่างยั่งยืน การบริหารความเสี่ยง ความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้การดำเนินธุรกิจของเครือเจริญโภคภัณฑ์เป็นไปตามหลักการกำกับดูแลกิจการที่ดี และตามกรอบยุทธศาสตร์และเป้าหมายการพัฒนาอย่างยั่งยืนของเครือฯ ปี 2030 เครือฯ จึงให้ความสำคัญกับการบริหารความเสี่ยงทั่วทั้งองค์กรและการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ รวมถึงมีการจัดหาอย่างยั่งยืนที่คำนึงถึงผลกระทบต่อสิ่งแวดล้อม ความรับผิดชอบต่อสังคม ชุมชน และธรรมชาติ (ESG) ซึ่งจะส่งผลให้การดำเนินธุรกิจของเครือฯ เป็นไปอย่างยั่งยืน

เครือฯ จึงทบทวนประกาศและนโยบายที่ประกาศใช้แล้วและปรับปรุงให้สอดคล้องกับมาตรฐานและแนวปฏิบัติที่ดีทั้งในประเทศและระดับสากล โดยเห็นสมควรยกเลิก

- ประกาศเครือเจริญโภคภัณฑ์ที่ คจก. 053/2561 ใช้ตั้งแต่วันที่ 1 พฤศจิกายน 2561 เรื่อง นโยบายและ แนวทางการบริหารความเสี่ยงทั่วทั้งองค์กร
 - นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ใช้ตั้งแต่วันที่ 27 กันยายน 2564 โดยให้ กรรมการ ผู้บริหาร และพนักงานเครือเจริญโภคภัณฑ์ ยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติ ดังนี้
 - นโยบายและแนวปฏิบัติด้านการบริหารความเสี่ยง เครือเจริญโภคภัณฑ์
 - นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เครือเจริญโภคภัณฑ์
 - นโยบายและแนวปฏิบัติด้านการจัดหาอย่างยั่งยืน เครือเจริญโภคภัณฑ์
- โดยมีรายละเอียดตามที่แนบท้ายประกาศ

ทั้งนี้ให้มีผลตั้งแต่วันที่ 1 เมษายน 2566 เป็นต้นไป

ประกาศ ณ วันที่ 1 เมษายน 2566

(นายสมชาย ไพบูรณ์พลาย้อย)
รองกรรมการผู้จัดการอาวุโส
ธุรกิจอุปการณ์การเกษตร



นโยบายและแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยสารสนเทศ
กลุ่มธุรกิจอุปกรณ์การเกษตร



รายการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
เครือข่ายธุรกิจ

ครั้งที่	ผู้รับผิดชอบ	สาระสำคัญ	ทบทวน โดย	อนุมัติ โดย	วันที่มีผล บังคับใช้
1					
2					

หมายเหตุ รายการปรับปรุงแก้ไขนโยบายเป็นเอกสารที่ใช้เพื่อการบริหารจัดการภายในเท่านั้น



รายการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
กลุ่มธุรกิจอุปกรณ์การเกษตร

ครั้งที่	ผู้รับผิดชอบ	สาระสำคัญ	ทบทวน โดย	อนุมัติ โดย	วันที่มีผล บังคับใช้
1					
2					

หมายเหตุ รายการปรับปรุงแก้ไขนโยบายเป็นเอกสารที่ใช้เพื่อการบริหารจัดการภายในเท่านั้น



สารบัญ

1. ความสำคัญ	1
2. ขอบเขตนโยบาย	1
3. วัตถุประสงค์	2
4. หน้าที่และความรับผิดชอบ	2
5. แนวปฏิบัติ	3
6. การฝึกอบรม	5
7. การแจ้งเบาะแส	5
8. การขอคำแนะนำ	5
9. บทลงโทษ	5
10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง	5
11. ภาคผนวก	6
ภาคผนวก ก คำนิยาม	7



นโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

กลุ่มธุรกิจอุปกรณ์การเกษตร

1. ความสำคัญ

กลุ่มธุรกิจอุปกรณ์การเกษตรตระหนักว่าสารสนเทศทั้งที่อยู่ในรูปแบบของเอกสารและอิเล็กทรอนิกส์ถือเป็นสินทรัพย์ที่มีค่าที่ใช้ในการดำเนินธุรกิจ ซึ่งอาจถูกจัดเก็บ รวบรวม ประมวลผลและส่งต่อผ่านระบบและเทคโนโลยีสารสนเทศควรได้รับการปกป้องจากการเข้าถึงที่ไม่ได้รับอนุญาต การเปิดเผย การดัดแปลงหรือการทำลายทำให้ไม่สามารถใช้งานต่อไปได้ และรักษาความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ กลุ่มธุรกิจอุปกรณ์การเกษตร จึงให้ความสำคัญในการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างเป็นระบบ มีประสิทธิภาพ ถูกต้อง สมบูรณ์และพร้อมใช้งาน เพื่อปกป้องสินทรัพย์ สารสนเทศ ป้องกันความเสี่ยงและลดความเสียหาย อันเกิดจากเหตุละเมิดความมั่นคงปลอดภัย รวมทั้งส่งเสริมให้เกิดความสามารถด้านการเตรียมพร้อมในการตอบสนองต่อภัยคุกคามทางไซเบอร์และการกู้คืนกระบวนการทางธุรกิจให้กลับมาดำเนินการได้ตามปกติ (Cyber Resilience) ตลอดจนตอบสนองความต้องการทางธุรกิจและกลุ่มผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทานภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ของบริษัท

กลุ่มธุรกิจอุปกรณ์การเกษตร จึงได้กำหนดนโยบายและแนวปฏิบัติฉบับนี้ขึ้น เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้มีการบริหารความเสี่ยง การปกป้องดูแล การติดตาม การเฝ้าระวัง การตรวจสอบและการควบคุมเป็นไปตามกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง โดยยึดหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งานของสินทรัพย์สารสนเทศ (Availability) และความปลอดภัย (Safety) เพื่อสร้างความต่อเนื่องในการดำเนินธุรกิจ ให้พนักงานทำงานด้วยความปลอดภัย สร้างวัฒนธรรมด้านความมั่นคงปลอดภัยที่เข้มแข็งและเพิ่มขีดความสามารถทางการแข่งขันอย่างยั่งยืน

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับเครือเจริญโภคภัณฑ์ ต่อไปนี้เรียกว่า “เครือฯ” หมายถึงบริษัท เครือเจริญโภคภัณฑ์ จำกัด และบริษัทในเครือทุกบริษัทที่บริษัท เครือเจริญโภคภัณฑ์ จำกัด มีอำนาจบริหาร ซึ่ง “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่ง ๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

- 3.1 เพื่อให้กรรมการ ผู้บริหาร และพนักงานมีแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
- 3.2 เพื่อป้องกันการเข้าถึงและใช้งานสินทรัพย์สารสนเทศให้มีความมั่นคงปลอดภัยจากความเสี่ยงด้านสารสนเทศที่อาจส่งผลกระทบต่อการดำเนินธุรกิจของบริษัท

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการบริษัท

- 4.1.1 พิจารณานุมัตินโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
- 4.1.2 กำกับดูแลให้การดำเนินธุรกิจเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ มาตรฐานและนโยบายและแนวปฏิบัติที่เกี่ยวข้อง
- 4.1.3 ติดตามดูแลให้เกิดการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

- 4.2.1 กำหนดกฎ ระเบียบ และขั้นตอนการดำเนินงานที่เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับกลยุทธ์ นโยบายและแนวปฏิบัติ
- 4.2.2 จัดให้มีโครงสร้างองค์กรที่มีผู้รับผิดชอบ และบทบาทหน้าที่ที่เหมาะสม
- 4.2.3 กำหนดแผนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งแผนบริหารความต่อเนื่องทางธุรกิจ
- 4.2.4 จัดให้มีระบบบริหารจัดการความเสี่ยง และการควบคุมภายใน
- 4.2.5 สื่อสารนโยบายและแนวปฏิบัติเพื่อสร้างการตระหนักรู้ให้กับผู้บริหารและพนักงานทุกระดับ
- 4.2.6 บริหารจัดการ และสนับสนุนให้มีการปฏิบัติตามกฎ ระเบียบ ขั้นตอนการดำเนินงาน และมาตรฐานที่เกี่ยวข้อง
- 4.2.7 จัดให้มีช่องทางติดต่อหน่วยงานหรือบุคคลผู้รับผิดชอบ เพื่อรับแจ้งเหตุในกรณีที่เกิดเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 4.2.8 ส่งเสริมให้เกิดวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ทั่วทั้งองค์กร
- 4.2.9 พิจารณารายงานผลการดำเนินงานและแนวทางในการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์อย่างสม่ำเสมอ

4.3 หน่วยงานหรือบุคคลผู้รับผิดชอบ

- 4.3.1 ประเมินและบริหารจัดการความเสี่ยงที่ครอบคลุมภัยคุกคาม (threat) ช่องโหว่ (vulnerability) ความเป็นไปได้ (likelihood) และผลกระทบ (impact) ต่อสินทรัพย์ ด้านสารสนเทศ และผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน
- 4.3.2 กำหนดมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ให้สอดคล้องตามนโยบายและแนวปฏิบัติ รวมทั้งขั้นตอนการดำเนินงานและมาตรฐานที่เกี่ยวข้อง
- 4.3.3 เผื่อระวังและบำรุงรักษาสินทรัพย์สารสนเทศให้อยู่ในสภาพพร้อมใช้งาน และมีความมั่นคงปลอดภัยอย่างต่อเนื่อง
- 4.3.4 ติดตามกฎหมาย ระเบียบ ข้อกำหนดและมาตรฐานต่าง ๆ ที่เกี่ยวข้องและนำมาปรับปรุงมาตรการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ รวมทั้งติดตามดูแลการปฏิบัติตามมาตรการที่กำหนดอย่างสม่ำเสมอ
- 4.3.5 กำหนดเกณฑ์และวิธีการรายงานเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 4.3.6 สร้างความตระหนักรู้และให้คำแนะนำแก่บุคลากร และผู้มีส่วนได้เสียทั้งภายในและภายนอก ตลอดห่วงโซ่อุปทาน
- 4.3.7 จัดทำรายงานผลการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

4.4 พนักงาน

- 4.4.1 เรียนรู้ ทำความเข้าใจและปฏิบัติตามกฎ ระเบียบ ข้อบังคับ นโยบายและแนวปฏิบัติ
- 4.4.2 ดำเนินการและรายงานเหตุการณ์ความผิดปกติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่ส่งผลกระทบต่อการใช้ปฏิบัติหน้าที่หรือเหตุการณ์ที่เกิดขึ้นตามช่องทางที่บริษัทกำหนด
- 4.4.3 ร้องเรียนหรือแจ้งเบาะแสเมื่อพบกรณีกระทำผิดหรือการกระทำที่อาจเข้าข่ายฝ่าฝืนนโยบายฉบับนี้

5. แนวปฏิบัติ

- 5.1 ประเมินและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ตามบริบททางธุรกิจและครอบคลุมความเสี่ยงที่เกิดจากผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน

- 5.2 จัดทำกลยุทธ์การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ที่สอดคล้องกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และระดับความเสี่ยงที่ยอมรับได้ของบริษัท
- 5.3 กำหนดแผนและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์โดยครอบคลุมการระบุบริบทสภาพแวดล้อมขององค์กร (identification) การปกป้องสินทรัพย์สารสนเทศ (protection) การตรวจจับเหตุการณ์ผิดปกติ (detection) การรับมือเหตุการณ์ผิดปกติ (response) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหาย (recovery)
- 5.4 บริหารจัดการสินทรัพย์สารสนเทศของบริษัทที่ดำเนินการทั้งโดยบุคลากรภายในและบุคคลภายนอกให้มีความมั่นคงปลอดภัยในทุกขั้นตอนของวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ (secure system / software development life cycle)
- 5.5 ปกป้องสารสนเทศและข้อมูลที่ส่งผ่านระบบและเทคโนโลยีสารสนเทศ ซึ่งรวมถึงข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้า และบริษัทที่รับผิดชอบประมวลผล ให้ปลอดภัยจากการเข้าถึงนำไปใช้ ส่งต่อ แก่ไข ทำซ้ำ ดัดแปลง ลบ หรือทำลายโดยไม่ได้รับอนุญาต
- 5.6 ตรวจสอบและปิดช่องโหว่ (vulnerability management) ของระบบและเทคโนโลยีสารสนเทศ รวมถึงดำเนินการปรับปรุงระบบให้มีความมั่นคงปลอดภัย (patch management) อย่างสม่ำเสมอ
- 5.7 เฝ้าระวัง (monitoring) และตรวจจับเหตุการณ์ความผิดปกติหรือเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบต่อความต่อเนื่องในการดำเนินธุรกิจ รวมทั้งตรวจสอบมาตรการที่เกี่ยวข้องให้มีประสิทธิภาพอย่างต่อเนื่อง
- 5.8 จัดให้มีกระบวนการบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์รวมทั้งปรับปรุงกระบวนการให้มีประสิทธิภาพอย่างสม่ำเสมอ สามารถจำกัดขอบเขต แก่ไข บรรเทาผลกระทบและเยียวยา รวมถึงการกู้คืนการดำเนินธุรกิจและสินทรัพย์สารสนเทศอย่างทันท่วงที มีความมั่นคงปลอดภัย
- 5.9 สนับสนุนและร่วมมือกับองค์กรภาคเอกชน ภาครัฐ และภาคประชาสังคมทั้งในประเทศและต่างประเทศในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 5.10 ส่งเสริมและสนับสนุนการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์แก่บุคลากร ลูกค้า คู่ค้า พันธมิตรและผู้มีส่วนได้เสียทั้งภายในและภายนอกตลอดห่วงโซ่อุปทาน

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ที่เหมาะสมให้แก่ กรรมการ ผู้บริหาร พนักงานและผู้มีส่วนได้เสียภายนอก ซึ่งรวมถึงคู่ค้า พันธมิตรทางธุรกิจ และสาธารณชน ตลอดห่วงโซ่อุปทาน รวมถึงจัดให้มีการประเมินประสิทธิผลหลังการฝึกอบรมทุกครั้ง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและแนวปฏิบัตินี้ โดยปฏิบัติตามแนวทางของนโยบายและแนวปฏิบัติด้านการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงาน ทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำ

ในกรณีที่ มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ สามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคล ผู้รับผิดชอบ ด้านกำกับปฏิบัติตามกฏเกณฑ์ ด้านระบบและเทคโนโลยีสารสนเทศ และด้านงานกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงาน

10. กฎหมาย ระเบียบและนโยบายที่เกี่ยวข้อง

- 10.1 กฎหมายที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
- 10.2 กฎหมายที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์



- 10.3 กฎหมายที่เกี่ยวกับคุ้มครองข้อมูลส่วนบุคคล
- 10.4 กฎหมายที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
- 10.5 มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)
- 10.6 กรอบความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework : CSF) ของ National Institute of Standards and Technology (NIST)
- 10.7 กรอบ Control Objectives for Information and Related Technologies (COBIT) ของ ISACA และ IT Governance Institute
- 10.8 CIS Controls ของศูนย์รักษาความปลอดภัยอินเทอร์เน็ต (Center for Internet Security: CIS)
- 10.9 กรอบการประเมินด้านไซเบอร์ (The Cyber Assessment Framework : CAF) ของศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร (National Cyber Security Centre : NCSC)

11. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

- 11.1 ภาคผนวก ก คำนิยาม

ภาคผนวก ก

คำนิยาม

1. การควบคุม (Control)

วิธีการจัดการ การปฏิบัติงาน หรือเทคนิคใด ๆ ที่ใช้ในการจัดการความเสี่ยง ซึ่งถูกออกแบบมาเพื่อติดตามและวัดผลตามมาตรฐานเฉพาะด้านนั้น ๆ เพื่อให้บริษัทสามารถบรรลุเป้าหมายหรือวัตถุประสงค์ที่กำหนดไว้

2. ความปลอดภัย (Safety)

การลดความเสี่ยงที่เกี่ยวกับเทคโนโลยี ซึ่งอาจมีความผิดพลาดหรือถูกควบคุมโดยผู้ประสงค์ร้ายที่ก่อให้เกิดความเสียหายต่อบุคคลและสินทรัพย์

3. ความมั่นคงปลอดภัย (Security)

กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาสินทรัพย์สารสนเทศที่สำคัญให้พ้นจากความพยายามใด ๆ ทั้งจากบุคลากรภายในและจากบุคคลภายนอก ในการเข้าถึงเพื่อโจรกรรม ทำลาย ทำให้เสียหาย หรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัทได้รับความเสียหาย โดยมีหลักการดังนี้

- ความลับ (confidentiality) การปกป้องความลับของสินทรัพย์สารสนเทศ โดยป้องกันการเข้าถึงและการเปิดเผยจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลที่เป็นกรรมสิทธิ์ของบริษัท
- ความถูกต้องครบถ้วน (integrity) การทำให้มั่นใจว่าสินทรัพย์สารสนเทศต้องไม่มีการแก้ไข ดัดแปลง หรือทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงสินทรัพย์สารสนเทศและบริการผ่านระบบทั้งออนไลน์และออฟไลน์ได้อย่างรวดเร็วและเชื่อถือได้
- ภาระรับผิดชอบ (accountability) การรับผิดชอบในผลของการกระทำ การสั่งการ การมอบหมาย และการตัดสินใจตามบทบาทหน้าที่ของตนเอง

- การพิสูจน์ตัวตน (authentication) การทำให้มั่นใจว่าสิทธิในการเข้าใช้งานสินทรัพย์สารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานสินทรัพย์สารสนเทศเป็นไปตามความจำเป็น (least privilege) และสอดคล้องกับความต้องการขั้นพื้นฐาน (need to know basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วมที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

4. ความมั่นคงปลอดภัยในวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ (Secure System/Software Development Life Cycle)

การกำหนดกระบวนการ มาตรการ และข้อกำหนดด้านความมั่นคงปลอดภัยให้เป็นส่วนหนึ่งของทุกขั้นตอนในวัฏจักรการพัฒนาระบบสารสนเทศ/ซอฟต์แวร์ ซึ่งครอบคลุมตั้งแต่การรวบรวมความต้องการ การออกแบบ การจัดหา การพัฒนา การทดสอบ การใช้งานและบำรุงรักษา รวมถึงการยกเลิกการใช้งาน

5. ความเสี่ยง

ผลกระทบเชิงลบที่เกิดจากเหตุการณ์ไม่แน่นอนต่อการบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน

6. ไซเบอร์

ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

7. เทคโนโลยีสารสนเทศ (Information Technology)

การประยุกต์ใช้เทคโนโลยีด้านคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ เครือข่ายด้านโทรคมนาคม และการสื่อสาร เพื่อค้นหา จัดเก็บ วิเคราะห์ ประมวลผล จัดส่ง กระจายออก ติดตาม รวบรวม และจัดการสารสนเทศต่าง ๆ ของบริษัท

8. ผู้มีส่วนได้เสีย (ภายในและภายนอก)

บุคคล กลุ่มบุคคล หรือหน่วยงานที่ได้รับผลกระทบจากการดำเนินงานของบริษัท ประกอบด้วยผู้มีส่วนได้เสียภายใน ได้แก่ กรรมการ ผู้บริหารและพนักงาน และผู้มีส่วนได้เสียภายนอก ได้แก่ ลูกค้า ผู้บริโภค คู่ค้าธุรกิจ พันธมิตรทางธุรกิจ ผู้ถือหุ้น นักลงทุน ชุมชน สังคม ภาครัฐ องค์กรพัฒนาเอกชน สื่อมวลชน คู่แข่งการค้าและเจ้าหนี้

9. พนักงาน (Employee)

พนักงานในระดับรองลงมาจากระดับผู้บริหารของบริษัทที่ได้รับการว่าจ้างให้เป็นพนักงานประจำ พนักงานทดลองงาน หรือพนักงานสัญญาจ้างพิเศษที่อยู่ภายใต้สัญญาจ้างของบริษัท

10. มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (Information and Cyber Security Measures)

มาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์แบ่งเป็น 5 ด้าน โดยครอบคลุมหัวข้อต่างๆ ดังนี้

- **การระบุสภาพแวดล้อมขององค์กร (identification)** ประกอบด้วย ธรรมภิบาล (governance) การบริหารจัดการความเสี่ยง (risk management) การกำกับปฏิบัติตามกฎเกณฑ์ (compliance) ความมั่นคงปลอดภัยด้านบุคลากร (human resource security) การบริหารจัดการความเสี่ยงในห่วงโซ่อุปทาน (supply chain risk management)
- **การปกป้องสินทรัพย์สารสนเทศ (protection)** ประกอบด้วย การบริหารจัดการสินทรัพย์สารสนเทศ (asset management) การควบคุมการเข้าถึงและการใช้งาน (access control) ความมั่นคงปลอดภัยในวัฏจักรการพัฒนา ระบบสารสนเทศ/ซอฟต์แวร์ (secure system/software development life cycle) การจัดการเข้ารหัสลับ (cryptographic management) ความมั่นคงปลอดภัยในการปฏิบัติงาน (operations security) การบริหารจัดการการเปลี่ยนแปลง (change management) การบริหารจัดการขีดความสามารถด้านสารสนเทศ (capacity and performance management) ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security) การบริหารจัดการการสื่อสารและการใช้งานระบบเครือข่าย (communication and network management)
- **การตรวจจับเหตุการณ์ผิดปกติ (detection)** ประกอบด้วย การบันทึกและการเฝ้าระวัง (log monitoring) การบริหารจัดการภัยคุกคาม (threat management)

- การรับมือเหตุการณ์ผิดปกติ (response) ประกอบด้วย การบริหารจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (information and cyber security incident management)
- การกู้คืนสินทรัพย์สารสนเทศจากความเสียหาย (recovery) ประกอบด้วย การบริหารความต่อเนื่องทางธุรกิจ (business continuity management) และการกู้คืนสินทรัพย์สารสนเทศจากความเสียหายให้กลับมาดำเนินการได้ตามปกติ (disaster recovery)

11. ระบบ (System)

สินทรัพย์ประเภทระบบหรือเครือข่ายที่สามารถกำหนด จำกัดขอบเขต และจัดการได้ รวมถึงคอมพิวเตอร์ เวิร์กสเตชัน แล็ปท็อป เซิร์ฟเวอร์ เราเตอร์ สวิตช์ ไฟร์วอลล์ อุปกรณ์สื่อสารแบบพกพา และเทคโนโลยีสารสนเทศอื่น ๆ เป็นต้น

12. สารสนเทศ (Information)

ข้อมูลของบริษัทที่ผ่านการประมวลผล วิเคราะห์ คำนวณ และมีการแปลความหมายที่อาจสามารถเข้าถึง ค้นหา หรือเรียกใช้งานผ่านระบบเครือข่ายอิเล็กทรอนิกส์หรือเทคโนโลยีการประมวลผลข้อมูลอิเล็กทรอนิกส์ต่าง ๆ ซึ่งอยู่ในทั้ง 2 รูปแบบ คือ

1. ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic information) ที่จัดเก็บอยู่ในระบบคอมพิวเตอร์หรือเกิดจากการให้บริการและการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต โครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน เช่น เอกสารอิเล็กทรอนิกส์ ฐานข้อมูล สื่อหรือโทรศัพท์ที่สามารถถอดออกได้ เครื่องมือที่ช่วยในการทำงานร่วมกัน เป็นต้น
2. ข้อมูลที่อยู่ในรูปแบบทางกายภาพ (Physical information) เช่น เอกสารที่พิมพ์ออกมา เป็นต้น

13. สินทรัพย์สารสนเทศ (Information Asset)

สารสนเทศ และระบบ รวมถึง ซอฟต์แวร์ แอปพลิเคชัน บริการ หรือทรัพยากรทางด้านสารสนเทศอื่น ๆ ที่สนับสนุนการดำเนินธุรกิจ และมีมูลค่าทางเศรษฐกิจต่อบริษัท

14. เหตุละเมิดความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ (ทั้งภายนอกและภายใน)

สถานการณ์หรือเหตุการณ์ใด ๆ ที่อาจส่งผลกระทบต่อการทำงานของปฏิบัติการหรือสินทรัพย์สารสนเทศของบริษัท บุคคล หรือองค์กรอื่นผ่านการเข้าถึงสินทรัพย์สารสนเทศ การทำลาย การเปิดเผย การแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และ/หรือการทำให้ไม่สามารถให้บริการได้