The NIST Cybersecurity Framework (CSF) 2.0

ดร.บรรจง หะรังษี

ผู้แปลและผู้เรียบเรียง

T-NET

Technology and

Cyber Security Services

ผู้นำด้านเทคโนโลยีและบริการด้านความมั่นคงปลอดภัย

ของคอมพิวเตอร์และระบบเครือข่าย

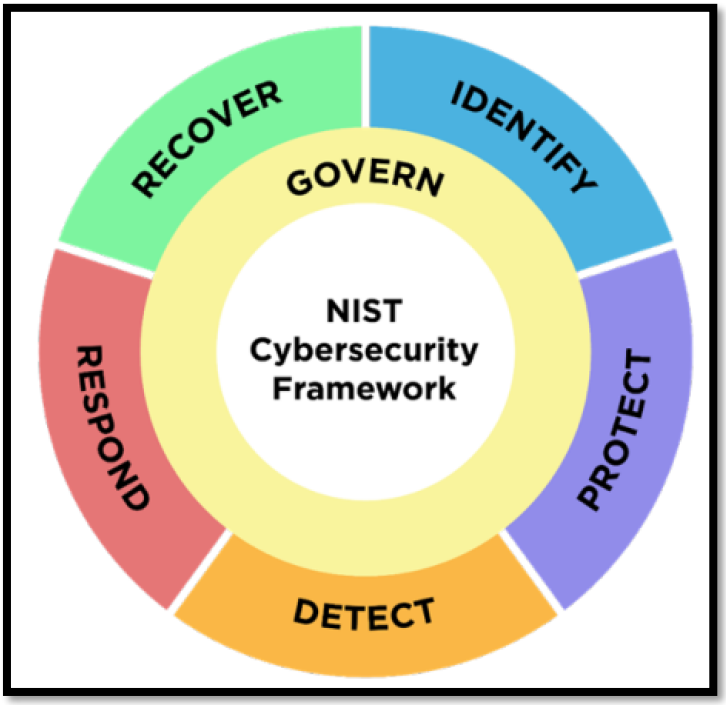
Tel. 02-564-7886 / Fax. 02-564-7854

info@tnetsecurity.com

121, Moo.9, Garden of Innovation Building
Thailand Science Park, Phahonyothin Rd.,
Klong 1, Klong Luang, Pathumthani
Thailand 12120

NIST CSF เวอร์ชั่น 2 มีแกนหลักประกอบด้วย 5 ฟังก์ชัน (Functions) ตามที่ปรากฏในรูป ได้แก่

- **Govern (GV)** - การกำกับดูแลการบริหารความเสี่ยง
- **Identify (ID)** - การระบุความเสี่ยง
- **Protect (PR)** - การป้องกันความเสี่ยง
- **Respond (RS)** – การรับมือกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (หรือจะเรียกว่าภัยคุกคามทางไซเบอร์ก็ได้)
- **Recover (RC)** - การกู้คืนจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น



แต่ละฟังก์ชันประกอบด้วยหมวดต่างๆ (Categories) ตามที่ปรากฏในตารางด้านล่าง

ฟังก์ชั่น (Function)	หมวด (Category)	ชื่อหมวด (Category Identifier)
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM

ฟังก์ชั่น (Function)	หมวด (Category)	ชื่อหมวด (Category Identifier)
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

แต่ละหมวด หรือ Category จะประกอบด้วยหมวดย่อยต่างๆ หรือที่เรียกว่า Subcategory ตามที่ปรากฏในส่วนสุดท้ายของเอกสารฉบับนี้ในหัวข้อ **ฟังก์ชั่น หมวด และหมวดย่อยในเอกสาร NIST CSF เวอร์ชั่น 2**

GOVERN (GV): กลยุทธ์ ความคาดหวัง และนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการกำหนด สื่อสาร และเฝ้าระวัง

- **Organizational Context (GV.OC):** สภาพแวดล้อม -- พันธกิจ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย บริการหรือระบบที่องค์กรจำเป็นต้องอาศัยการมีอยู่ของบริการหรือระบบเหล่านั้น กฎหมาย ระเบียบ ข้อบังคับ และสิ่งที่กำหนดไว้ในสัญญาจ้างที่องค์กรต้องปฏิบัติตาม
  - **GV.OC-01:** พันธกิจขององค์กรมีการทำความเข้าใจและสื่อสารหรือแจ้งให้ทราบถึงการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - **GV.OC-02:** ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกมีการกำหนด ตลอดจนความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียเหล่านั้นที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - **GV.OC-03:** ความต้องการหรือข้อกำหนดที่เกี่ยวข้องกับกฎหมาย ระเบียบ ข้อบังคับ และสิ่งที่กำหนดไว้ในสัญญาจ้างที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึง

การรักษาความเป็นส่วนตัวและการรักษาไว้ถึงสิทธิและเสรีภาพของผู้อื่น ต้องมีการทำความเข้าใจและบริหารจัดการความต้องการหรือข้อกำหนดเหล่านั้น

- **GV.OC-04:** วัตถุประสงค์ ขีดความสามารถ และบริการที่มีความสำคัญ ซึ่งมีผู้มีส่วนได้ส่วนเสียภายนอกจำเป็นต้องพึ่งพาอาศัยจากองค์กร ต้องมีการทำความเข้าใจและสื่อสารให้เป็นที่ทราบกัน
- **GV.OC-05:** ผลลัพธ์ ขีดความสามารถ และบริการที่องค์กรจำเป็นต้องพึ่งพาอาศัย ต้องมีการทำความเข้าใจและสื่อสารให้เป็นที่ทราบกัน

- **Risk Management Strategy (GV.RM):** ลำดับความสำคัญ ข้อจำกัด ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ระดับความเบี่ยงเบนความเสี่ยง (Risk Tolerance) และสมมติฐานต่างๆ ขององค์กร ต้องมีการทำความเข้าใจ สื่อสารให้เป็นที่ทราบกัน และใช้เป็นข้อมูลในการสนับสนุนการตัดสินใจดำเนินการต่างๆ ที่เกี่ยวข้องกับการบริหารความเสี่ยง
  - **GV.RM-01:** วัตถุประสงค์ของการบริหารความเสี่ยงต้องมีการกำหนดและรับรองโดยผู้มีส่วนได้ส่วนเสียขององค์กร
  - **GV.RM-02:** ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และระดับความเบี่ยงเบนความเสี่ยง (Risk Tolerance) ต้องมีการกำหนด สื่อสารให้เป็นที่ทราบกัน และปรับปรุงตามความจำเป็น
  - **GV.RM-03:** กิจกรรมและผลลัพธ์การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องปรากฏอยู่ในกระบวนการบริหารความเสี่ยงระดับองค์กร
  - **GV.RM-04:** ทิศทางเชิงกลยุทธ์ที่กล่าวถึงทางเลือกในการจัดการกับความเสี่ยงอย่างเหมาะสมต้องมีการกำหนดและสื่อสารให้เป็นที่ทราบกัน
  - **GV.RM-05:** ช่องทางการสื่อสารทั่วทั้งองค์กรต้องมีการกำหนดสำหรับการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากผู้ให้บริการภายนอกและผู้มีส่วนได้ส่วนเสียอื่นๆ
  - **GV.RM-06:** วิธีการบริหารความเสี่ยงที่เป็นมาตรฐานสำหรับการคำนวณ บันทึกข้อมูล จัดหมวดหมู่ และจัดลำดับความสำคัญของความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการกำหนดและสื่อสารให้เป็นที่ทราบกัน

- **Roles, Responsibilities, and Authorities (GV.RR):** บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่เพื่อสนับสนุนความรับผิดชอบ การประเมินผล และการปรับปรุงอย่างต่อเนื่องสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีการกำหนดและสื่อสารให้เป็นที่ทราบกัน
  - **GV.RR-01:** ผู้บริหารสูงสุดต้องมีภาวะผู้นำและต้องรับผิดชอบในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งสนับสนุนวัฒนธรรมที่มีการตระหนักถึงความเสี่ยง จริยธรรมคุณธรรม และการปรับปรุงอย่างต่อเนื่อง

- **GV.RR-02:** บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการกำหนด สื่อสารให้เป็นที่ทราบกัน ทำความเข้าใจ และบังคับใช้
- **GV.RR-03:** ทรัพยากรต้องมีการจัดสรรอย่างเพียงพอและเป็นสัดส่วนกับกลยุทธ์การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ บทบาท หน้าที่ความรับผิดชอบ และนโยบายที่เกี่ยวข้อง
- **GV.RR-04:** การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องเป็นส่วนหนึ่งในวิธีปฏิบัติด้านบุคลากรขององค์กร

- **Policy (GV.PO):** นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรต้องมีการกำหนด สื่อสารให้เป็นที่ทราบกัน และบังคับใช้
  - **GV.PO-01:** นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการกำหนด โดยพิจารณาจากบริบทขององค์กร กลยุทธ์การรักษาความมั่นคงปลอดภัยไซเบอร์ และลำดับของสิ่งสำคัญที่องค์กรต้องดำเนินการ มีการสื่อสารให้เป็นที่ทราบกันและบังคับใช้
  - **GV.PO-02:** นโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการทบทวน ปรับปรุง สื่อสารให้เป็นที่ทราบกัน และบังคับใช้เพื่อสะท้อนถึงการเปลี่ยนแปลงด้านความต้องการ ภัยคุกคาม และพันธกิจขององค์กร
- **Oversight (GV.OV):** ผลของการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั่วทั้งองค์กร และประสิทธิภาพในการดำเนินการต้องมีการใช้ประโยชน์ เพื่อแจ้งให้ทราบหรือบอกให้รู้ และปรับปรุงกลยุทธ์การบริหารความเสี่ยงขององค์กร
  - **GV.OV-01:** ผลลัพธ์ของกลยุทธ์การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการทบทวนเพื่อแจ้งให้ทราบหรือบอกให้รู้ และปรับปรุงกลยุทธ์และทิศทางขององค์กร
  - **GV.OV-02:** กลยุทธ์การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการทบทวนและปรับปรุงเพื่อให้มั่นใจว่าครอบคลุมความต้องการและความเสี่ยงขององค์กร
  - **GV.OV-03:** ประสิทธิภาพในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรต้องมีการประเมินและทบทวนเพื่อปรับปรุงตามความจำเป็น
- **Cybersecurity Supply Chain Risk Management (GV.SC):** กระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในห่วงโซ่การให้บริการของผู้ให้บริการภายนอก ต้องมีการกำหนด บริหารจัดการ เฝ้าระวัง และปรับปรุงโดยผู้มีส่วนได้ส่วนเสียขององค์กร
  - **GV.SC-01:** โปรแกรม กลยุทธ์ วัตถุประสงค์ นโยบาย และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในห่วงโซ่การให้บริการของผู้ให้บริการภายนอกต้องมีการกำหนดและรับรองโดยผู้มีส่วนได้ส่วนเสียขององค์กร

- **GV.SC-02:** บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก ลูกค้า และหุ้นส่วน ต้องมีการกำหนด สื่อสารให้เป็นที่ทราบกัน และประสานงานกันทั้งภายในและภายนอก
- **GV.SC-03:** การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในห่วงโซ่การให้บริการของผู้ให้บริการภายนอกต้องมีบูรณาการเข้ากับการรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยงระดับองค์กร การประเมินความเสี่ยง และกระบวนการปรับปรุงให้ดียิ่งขึ้น
- **GV.SC-04:** ผู้ให้บริการภายนอกต้องมีการกำหนดและจัดลำดับตามความสำคัญของผู้ให้บริการภายนอก
- **GV.SC-05:** ความต้องการหรือข้อกำหนดเพื่อจัดการกับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในห่วงโซ่ของการให้บริการต้องมีการกำหนด จัดลำดับความสำคัญ และบรรจุเข้าไปในสัญญาจ้างและข้อตกลงอื่นๆ กับผู้ให้บริการภายนอกที่เกี่ยวข้อง
- **GV.SC-06:** การวางแผนและการใช้ความระมัดระวังอย่างรอบคอบต้องมีการปฏิบัติเพื่อลดความเสี่ยงต่างๆ ก่อนการเริ่มต้นการปฏิบัติงานกับผู้ให้บริการภายนอกอย่างเป็นทางการ
- **GV.SC-07:** ความเสี่ยงที่มาจากผู้ให้บริการภายนอก ผลิตภัณฑ์และบริการของผู้ให้บริการภายนอก และผู้มีส่วนได้ส่วนเสียอื่นๆ ที่เกี่ยวข้อง ต้องมีการทำความเข้าใจ บันทึก จัดลำดับความสำคัญ ประเมิน รับมือ และเฝ้าระวังอย่างต่อเนื่องในช่วงที่มีการปฏิบัติงานกับผู้ให้บริการภายนอก
- **GV.SC-08:** ผู้ให้บริการภายนอกและผู้มีส่วนได้ส่วนเสียอื่นๆ ที่เกี่ยวข้อง ต้องนำมาพิจารณาเพื่อวางแผนกิจกรรมการรับมือและการกู้คืนจากภัยคุกคามทางไซเบอร์
- **GV.SC-09:** วิธีปฏิบัติด้านความมั่นคงปลอดภัยในห่วงโซ่การให้บริการของผู้ให้บริการภายนอกต้องมีการผนวกเข้ากับการรักษาความมั่นคงปลอดภัยไซเบอร์ และโปรแกรมบริหารจัดการความเสี่ยงระดับองค์กร ประสิทธิภาพของการปฏิบัติต้องมีการเฝ้าระวังอย่างต่อเนื่องตลอดวงจรชีวิตของบริการและผลิตภัณฑ์ด้านเทคโนโลยีนั้น
- **GV.SC-10:** แผนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในห่วงโซ่การให้บริการ ต้องรวมถึงกิจกรรมที่เกิดขึ้นหลังสิ้นสุดความสัมพันธ์หรือข้อตกลงการให้บริการกับผู้ให้บริการภายนอก

IDENTIFY (ID): ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรในปัจจุบันต้องมีการทำความเข้าใจ

- **Asset Management (ID.AM):** ทรัพย์สิน เช่น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ ระบบ สิ่งอำนวยความสะดวก บริการ และบุคลากร ที่ทำให้องค์กรบรรลุจุดประสงค์ทางธุรกิจ ต้องมีการระบุและ

บริหารจัดการ ให้สอดคล้องกับความสำคัญโดยเปรียบเทียบของทรัพย์สินเหล่านั้นเทียบกับวัตถุประสงค์และกลยุทธ์ด้านความเสี่ยงขององค์กร

- **ID.AM-01:** บัญชีทรัพย์สินด้านฮาร์ดแวร์บริหารจัดการโดยองค์กรต้องมีการจัดทำและปรับปรุง
- **ID.AM-02:** บัญชีทรัพย์สินด้านซอฟต์แวร์ บริการ และระบบ ที่มีการบริหารจัดการโดยองค์กร ต้องมีการจัดทำและปรับปรุง
- **ID.AM-03:** แผนผังแสดงการสื่อสารผ่านทางระบบเครือข่ายที่ได้รับอนุญาต และแผนผังแสดงการไหลของข้อมูลผ่านเครือข่ายทั้งภายในและภายนอกต้องมีการจัดทำและปรับปรุง
- **ID.AM-04:** บัญชีทรัพย์สินด้านบริการที่มีการให้บริการโดยผู้ให้บริการภายนอกต้องมีการจัดทำและปรับปรุง
- **ID.AM-05:** ทรัพย์สินต้องมีการจัดลำดับความสำคัญโดยพิจารณาจากชั้นความลับ ความสำคัญ ทรัพยากรที่ใช้ และผลกระทบที่มีต่อพันธกิจขององค์กร
- **ID.AM-07:** บัญชีทรัพย์สินด้านข้อมูลและ Metadata ที่เกี่ยวข้องต้องมีการจัดทำและปรับปรุง
- **ID.AM-08:** ระบบ ฮาร์ดแวร์ ซอฟต์แวร์ บริการ และข้อมูลต้องมีการบริหารจัดการตลอดวงจรชีวิตของทรัพย์สินเหล่านั้น

- **Risk Assessment (ID.RA):** ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อองค์กร ทรัพย์สิน และบุคคลากร ต้องมีการศึกษาและทำความเข้าใจ
  - **ID.RA-01:** จุดอ่อนหรือช่องโหว่ในทรัพย์สินต้องมีการระบุ ตรวจสอบความถูกต้อง และบันทึกไว้
  - **ID.RA-02:** การข่าวด้านภัยคุกคามทางไซเบอร์ ต้องได้รับจาก forum และแหล่งต่างๆ ที่มีการแชร์ข้อมูลข่าวสารให้
  - **ID.RA-03:** ภัยคุกคามทั้งภายในและภายนอกที่มีต่อองค์กรต้องมีการระบุและบันทึกไว้
  - **ID.RA-04:** ผลกระทบและโอกาสเกิดขึ้นของภัยคุกคามทางไซเบอร์ที่ใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ ต้องมีการระบุและบันทึกไว้
  - **ID.RA-05:** ภัยคุกคามทางไซเบอร์ จุดอ่อนหรือช่องโหว่ โอกาสการเกิดขึ้น และผลกระทบต้องถูกใช้เพื่อทำความเข้าใจความเสี่ยงที่เป็นอยู่และใช้ในการจัดลำดับความสำคัญเพื่อรับมือกับความเสี่ยงนั้น
  - **ID.RA-06:** การรับมือกับความเสี่ยงต้องมีการกำหนด จัดลำดับความสำคัญ วางแผนติดตาม และสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ
  - **ID.RA-07:** การเปลี่ยนแปลงที่มีต่อบริบทขององค์กรต้องมีการบริหารจัดการและประเมินสำหรับผลกระทบที่มีต่อความเสี่ยง มีการบันทึกและติดตามผล

- **ID.RA-08:** กระบวนการสำหรับการรับ การวิเคราะห์ และการรับมือกับจุดอ่อนหรือช่องโหว่ต้องมีการกำหนด
- **ID.RA-09:** การประเมินฮาร์ดแวร์และซอฟต์แวร์ เพื่อดูความครบถ้วน ถูกต้อง รวมทั้งเป็นของแท้ ต้องมีการดำเนินการก่อนการใช้งาน
- **ID.RA-10:** การประเมินผู้ให้บริการภายนอกที่สำคัญต้องมีการดำเนินการ ก่อนการได้มาซึ่งผู้รับจ้างที่เหมาะสม

- **Improvement (ID.IM):** การปรับปรุงต่อกระบวนการ ขั้นตอนปฏิบัติ และกิจกรรมที่เกี่ยวข้องกับการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร ต้องมีการระบุและดำเนินการกับฟังก์ชันของ CSF ทั้งหมด
  - **ID.IM-01:** การปรับปรุงต้องมีการระบุและดำเนินการจากผลการประเมินต่างๆ
  - **ID.IM-02:** การปรับปรุงต้องมีการระบุและดำเนินการจากผลการทดสอบและการซ้อมด้านความมั่นคงปลอดภัย ซึ่งรวมถึงผลที่ดำเนินการร่วมกับผู้ให้บริการภายนอกและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
  - **ID.IM-03:** การปรับปรุงต้องมีการระบุและดำเนินการจากการปฏิบัติกับกระบวนการ ขั้นตอนปฏิบัติ และกิจกรรมต่างๆ
  - **ID.IM-04:** แผนการรับมือกับภัยคุกคามทางไซเบอร์ และแผนการรักษาความมั่นคงปลอดภัยไซเบอร์อื่นๆ ที่มีผลกระทบต่อการดำเนินงานขององค์กร ต้องมีการจัดทำ สื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ แก้ไข และปรับปรุงตามความจำเป็น

PROTECT (PR): มาตรการป้องกันเพื่อบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีการนำมาใช้งาน

- **Identity Management, Authentication, and Access Control (PR.AA):** การเข้าถึงทรัพย์สินทางกายภาพและใช้การล็อกอินเพื่อเข้าถึง ต้องมีการจำกัดให้เฉพาะผู้ใช้งาน บริการ และฮาร์ดแวร์ที่ได้รับอนุญาตแล้วเท่านั้น และต้องมีการบริหารจัดการอย่างเป็นสัดส่วนกับความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาตตามที่ประเมิน
  - **PR.AA-01:** อัตลักษณ์และข้อมูลการพิสูจน์ตัวตนสำหรับผู้ใช้งาน บริการ และฮาร์ดแวร์ที่ได้รับอนุญาตแล้ว ต้องมีการบริหารจัดการโดยองค์กร
  - **PR.AA-02:** อัตลักษณ์ต้องมีการพิสูจน์และเชื่อมโยงได้กับข้อมูลการพิสูจน์ตัวตนตามบริบทของการเข้าถึง
  - **PR.AA-03:** ผู้ใช้งาน บริการ และฮาร์ดแวร์ต้องมีการพิสูจน์ตัวตน
  - **PR.AA-04:** การยืนยันอัตลักษณ์ต้องมีการป้องกัน ซึ่งรวมถึงการถ่ายโอนและการตรวจสอบให้มีความถูกต้อง
  - **PR.AA-05:** การขออนุมัติการเข้าถึง การให้สิทธิ์ และการอนุมัติการเข้าถึง ต้องมีการกำหนดในนโยบาย มีการบริหารจัดการ บังคับใช้นโยบาย ตลอดจนทบทวนอย่างสม่ำเสมอ โดยต้อง

รวมหลักการให้สิทธิ์การเข้าถึงน้อยที่สุด และหลักการแยกหน้าที่ความรับผิดชอบออกจากกัน

- **PR.AA-06:** การเข้าถึงทางกายภาพต่อทรัพย์สินขององค์กรต้องมีการบริหารจัดการ เฝ้าระวัง และบังคับใช้ให้เป็นไปตามที่กำหนดตามสัดส่วนของความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง

- **Awareness and Training (PR.AT):** บุคลากรขององค์กรต้องได้รับการสร้างความตระหนักและการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถปฏิบัติหน้าที่หรือปฏิบัติงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ได้
  - **PR.AT-01:** บุคลากรขององค์กรต้องได้รับการสร้างความตระหนักและการฝึกอบรม เพื่อให้มีความรู้และทักษะในการปฏิบัติหน้าที่ที่มีความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
  - **PR.AT-02:** บุคลากรที่มีบทบาทเฉพาะต้องได้รับการสร้างความตระหนักและการฝึกอบรมเพื่อให้มีความรู้และทักษะในการปฏิบัติหน้าที่ที่มีความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- **Data Security (PR.DS):** ข้อมูลต้องได้รับการบริหารจัดการให้สอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อป้องกันความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลขององค์กร
  - **PR.DS-01:** ความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลที่มีการจัดเก็บไว้ ต้องได้รับการป้องกัน
  - **PR.DS-02:** ความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลที่มีการถ่ายโอนไปยังอีกที่หนึ่ง ต้องได้รับการป้องกัน
  - **PR.DS-10:** ความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลที่มีการใช้งาน ต้องได้รับการป้องกัน
  - **PR.DS-11:** ข้อมูลต้องมีการสำรองเก็บไว้ ต้องมีการป้องกัน การบำรุงรักษา (ให้สามารถใช้งานได้) และการทดสอบเพื่อให้มั่นใจว่าสามารถใช้งานได้
- **Platform Security (PR.PS):** ฮาร์ดแวร์ ซอฟต์แวร์ (เช่น Firmware ระบบปฏิบัติการ และ Application) และบริการต่างๆ ต้องได้รับการบริหารจัดการให้สอดคล้องกับกลยุทธ์ด้านความเสี่ยงขององค์กร ทั้งนี้เพื่อป้องกันความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลขององค์กร
  - **PR.PS-01:** วิธีปฏิบัติในการบริหารจัดการการตั้งค่า (Configuration management practices) ต้องมีการกำหนดและประยุกต์ใช้งาน
  - **PR.PS-02:** ซอฟต์แวร์ต้องมีการบำรุงรักษา เปลี่ยนทดแทน และจำหน่ายออก ให้เป็นสัดส่วนกับความเสี่ยงที่เกี่ยวข้อง
  - **PR.PS-03:** ฮาร์ดแวร์ต้องมีการบำรุงรักษา เปลี่ยนทดแทน และจำหน่ายออก ให้เป็นสัดส่วนกับความเสี่ยงที่เกี่ยวข้อง

- **PR.PS-04:** ข้อมูลล็อกต้องมีการสร้างและจัดเตรียมไว้ให้พร้อมใช้งานสำหรับการเฝ้าระวังอย่างต่อเนื่อง
- **PR.PS-05:** การติดตั้งและใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตต้องได้รับการป้องกัน
- **PR.PS-06:** วิธีปฏิบัติในการพัฒนาซอฟต์แวร์ให้มีความมั่นคงปลอดภัย ต้องมีการผนวกรวมเข้ากับการพัฒนาซอฟต์แวร์ ประสิทธิภาพของซอฟต์แวร์ต้องได้รับการเฝ้าระวังตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์

- **Technology Infrastructure Resilience (PR.IR):** สถาปัตยกรรมด้านความมั่นคงปลอดภัยต้องได้รับการบริหารจัดการให้สอดคล้องกับกลยุทธ์ด้านความเสี่ยงขององค์กรเพื่อป้องกันความลับ ความถูกต้อง และความพร้อมใช้ของทรัพย์สินขององค์กร ตลอดจนมีความยืดหยุ่นที่จะสามารถรับมือกับทั้งภัยคุกคามทางไซเบอร์และภัยพิบัติต่างๆ ได้
  - **PR.IR-01:** เครือข่ายและสภาพแวดล้อมขององค์กรต้องได้รับการป้องกันจากการเข้าถึงและใช้งานโดยไม่ได้รับอนุญาต
  - **PR.IR-02:** ทรัพย์สินที่เป็นเทคโนโลยีขององค์กรต้องได้รับการป้องกันจากภัยคุกคามด้านสภาพแวดล้อมขององค์กร
  - **PR.IR-03:** กลไกต่างๆ ต้องมีการเตรียมการและจัดทำเพื่อให้สามารถบรรลุความต้องการด้านความยืดหยุ่นที่จะทำให้สามารถรับมือกับทั้งภัยคุกคามทางไซเบอร์และภัยพิบัติต่างๆ ได้ ทั้งในสถานการณ์ปกติและไม่ปกติ
  - **PR.IR-04:** ทรัพยากรที่เพียงพอต้องมีการดูแลและปรับปรุงเพื่อให้มั่นใจด้านความพร้อมใช้

DETECT (DE): การโจมตีความมั่นคงปลอดภัยไซเบอร์ขององค์กรต้องมีการตรวจพบและวิเคราะห์

- **Continuous Monitoring (DE.CM):** ทรัพย์สินต้องมีการเฝ้าระวังเพื่อตรวจหาความผิดปกติ IoC (indicators of compromise ซึ่งหมายถึงสิ่งบ่งชี้ว่าระบบอาจจะถูกละเมิดความปลอดภัย) และเหตุการณ์ที่ผิดปกติอื่นๆ
  - **DE.CM-01:** เครือข่ายและบริการด้านเครือข่ายต้องได้รับการเฝ้าระวังเพื่อตรวจหาเหตุการณ์ผิดปกติต่างๆ
  - **DE.CM-02:** สภาพแวดล้อมทางกายภาพต้องได้รับการเฝ้าระวังเพื่อตรวจหาเหตุการณ์ผิดปกติต่างๆ
  - **DE.CM-03:** กิจกรรมของบุคลากรและการใช้งานเทคโนโลยีต้องได้รับการเฝ้าระวังเพื่อตรวจหาเหตุการณ์ผิดปกติต่างๆ
  - **DE.CM-06:** กิจกรรมและบริการของผู้ให้บริการภายนอกต้องได้รับการเฝ้าระวังเพื่อตรวจหาเหตุการณ์ผิดปกติต่างๆ
  - **DE.CM-09:** ฮาร์ดแวร์ ซอฟต์แวร์ สภาพแวดล้อม และข้อมูลของฮาร์ดแวร์และซอฟต์แวร์ดังกล่าวต้องได้รับการเฝ้าระวังเพื่อตรวจหาเหตุการณ์ผิดปกติต่างๆ

- **Adverse Event Analysis (DE.AE):** ความผิดปกติ IoC และเหตุการณ์ที่ผิดปกติอื่นๆ ต้องได้รับการวิเคราะห์เพื่อกำหนดคุณลักษณะของเหตุการณ์ และตรวจจับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
  - **DE.AE-02:** เหตุการณ์ผิดปกติต้องได้รับการวิเคราะห์เพื่อทำความเข้าใจในกิจกรรมต่างๆ ที่เกี่ยวข้อง (จากเหตุการณ์ดังกล่าว)
  - **DE.AE-03:** ข้อมูลจากหลายๆ แหล่งต้องนำมาวิเคราะห์และหาความสัมพันธ์กัน
  - **DE.AE-04:** ผลกระทบและขอบเขตของเหตุการณ์ผิดปกติต้องได้รับการประเมินเพื่อทำความเข้าใจ
  - **DE.AE-06:** ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ผิดปกติ ต้องมีการจัดเตรียมให้แก่บุคลากรและเครื่องมือ (สำหรับการวิเคราะห์ต่างๆ) ที่ได้รับอนุญาต
  - **DE.AE-07:** การข่าวด้านภัยคุกคามทางไซเบอร์ และข้อมูลจากบริบทอื่นๆ ต้องนำมาผนวกรวมเข้ากับการวิเคราะห์
  - **DE.AE-08:** เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการประกาศเมื่อเหตุการณ์ผิดปกติที่พบมีความสอดคล้องกับเกณฑ์การประเมินเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้

RESPOND (RS): การดำเนินการที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบต้องมีการลงมือปฏิบัติ

- **Incident Management (RS.MA):** การรับมือกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบต้องมีการบริหารจัดการ
  - **RS.MA-01:** แผนการรับมือกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการปฏิบัติร่วมกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทันทีที่เหตุการณ์ดังกล่าวได้รับการประกาศ
  - **RS.MA-02:** รายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการจัดเตรียมและตรวจสอบความถูกต้องตามระดับความรุนแรงหรือผลกระทบของเหตุการณ์
  - **RS.MA-03:** เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการจัดหมวดหมู่และลำดับความสำคัญในการดำเนินการ
  - **RS.MA-04:** เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องมีการประสานงานส่งต่อหรือยกระดับความรุนแรงตามความจำเป็น ไปยังผู้บังคับบัญชาและผู้ที่เกี่ยวข้อง
  - **RS.MA-05:** เกณฑ์การกำหนดให้ต้องมีการกู้คืนต้องมีการกำหนด
- **Incident Analysis (RS.AN):** การสอบสวนต้องมีการดำเนินการ เพื่อให้มั่นใจถึงการรับมืออย่างได้ผลและสนับสนุนกิจกรรมการกู้คืนและนิติวิทยาศาสตร์ที่เกี่ยวข้อง
  - **RS.AN-03:** การวิเคราะห์ต้องมีการดำเนินการเพื่อกำหนดสิ่งที่เกิดขึ้นและหาสาเหตุพื้นฐานของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น

- **RS.AN-06:** การดำเนินการต่างๆ ในช่วงที่มีการสอบสวน ต้องมีการบันทึกไว้และคงไว้ซึ่งความถูกต้องของบันทึกและข้อมูลต่างๆ รวมทั้งแหล่งที่มา
- **RS.AN-07:** ข้อมูลที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ต้องมีการเก็บรวบรวม และต้องคงไว้ซึ่งความถูกต้องและแหล่งที่มาของข้อมูลเหล่านั้น
- **RS.AN-08:** ผลกระทบหรือความรุนแรงของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ต้องได้รับการประเมินและตรวจสอบความถูกต้อง

- **Incident Response Reporting and Communication (RS.CO):** กิจกรรมการรับมือต้องมีการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องตามที่กฎหมาย ระเบียบข้อบังคับ หรือนโยบายกำหนดไว้
  - **RS.CO-02:** ผู้มีส่วนใดส่วนเสียทั้งภายในและภายนอกต้องได้รับการแจ้งเตือนถึงเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น
  - **RS.CO-03:** ข้อมูลต้องได้รับการแชร์กับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่กำหนดไว้
- **Incident Mitigation (RS.MI):** การดำเนินการต่างๆ ต้องมีการลงมือปฏิบัติเพื่อป้องกันการกระจายตัวและลดผลกระทบของเหตุการณ์ที่เกิดขึ้น
  - **RS.MI-01:** เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ต้องได้รับการจำกัดไม่ให้มีการกระจายตัว
  - **RS.MI-02:** เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ต้องได้รับการค้นหาสาเหตุเพื่อถอนรากถอนโคนของเหตุที่เกิดขึ้น

RECOVER (RC): ทรัพย์สินและการดำเนินงานต่างๆ ขององค์กรที่ได้รับผลกระทบจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ต้องได้รับการกู้คืน

- **Incident Recovery Plan Execution (RC.RP):** กิจกรรมการกู้คืนต้องได้รับการดำเนินการเพื่อให้มั่นใจในความพร้อมใช้ของระบบและบริการต่างๆ ที่ได้รับผลกระทบจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
  - **RC.RP-01:** ส่วนของการกู้คืนในแผนการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ต้องได้รับการปฏิบัติทันทีที่กระบวนการรับมือกำหนดให้ต้องดำเนินการกู้คืน
  - **RC.RP-02:** การดำเนินการกู้คืนต้องมีการกำหนด จำกัดขอบเขต จัดลำดับสิ่งที่ต้องดำเนินการ และลงมือปฏิบัติ
  - **RC.RP-03:** ความถูกต้องและความครบถ้วนของข้อมูลสำรองและทรัพย์สินที่ใช้ในการกู้คืนอื่นๆ ต้องได้รับการประเมินก่อนที่จะใช้ข้อมูลและทรัพย์สินเหล่านั้นในการกู้คืน
  - **RC.RP-04:** ฟังก์ชั่นที่มีความสำคัญต่อองค์กร และการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีการพิจารณาเพื่อกำหนดมาตรฐานขั้นต่ำของการดำเนินงานภายหลังการกู้คืน

- **RC.RP-05:** ความถูกต้องและความครบถ้วนของทรัพย์สินที่ได้รับการกู้คืนต้องได้รับการตรวจสอบ ระบบและบริการต้องได้รับการกู้คืน และสถานะของการให้บริการได้ตามปกติต้องได้รับการยืนยัน
- **RC.RP-06:** การสิ้นสุดของกิจกรรมการกู้คืนต้องมีการประกาศตามเกณฑ์ที่กำหนดไว้ และการจัดทำเอกสารต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ที่เกิดขึ้นต้องได้รับการจัดทำโดยสมบูรณ์

- **Incident Recovery Communication (RC.CO):** กิจกรรมการกู้คืนต้องได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก
  - **RC.CO-03:** กิจกรรมการกู้คืนและความคืบหน้าของการกู้คืนต้องได้รับการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่กำหนดไว้
  - **RC.CO-04:** การอัพเดทข้อมูลเพื่อให้สาธารณะได้รับทราบต้องมีการดำเนินการโดยใช้วิธีการและช่องทางการส่งข้อมูลข่าวสารที่องค์กรกำหนดไว้