



**นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ**

## 1. ความสำคัญ (Intent)

นโยบายรักษาความปลอดภัยข้อมูล สารสนเทศ (ISP) กำหนดให้โครงสร้าง เพื่อการวัดผลและปรับปรุง การรักษา ความลับ ความสมบูรณ์ ความพร้อมใช้งาน (CIA) และความสอดคล้องกัน เพื่อปฏิบัติตามคำสั่งและแนวทางความยั่งยืนของเครือเจริญโภคภัณฑ์ (“เครือซีพี”) และเป็นนโยบายและมาตรฐานต่อบริษัท ซีพี แอ็กซ์ตรา จำกัด (มหาชน) และบริษัทย่อย (“เครือซีพี แอ็กซ์ตรา”)

## 2. วัตถุประสงค์ (Objectives)

- นโยบายการรักษา ความปลอดภัยของข้อมูล สารสนเทศ และแนวทางที่ครอบคลุมสำหรับ กลุ่ม ซีพี แอ็กซ์ตรา ในการจัดการข้อมูลและระบบทั่วทั้งองค์กร ในลักษณะที่สอดคล้องและมีประสิทธิภาพ ซึ่งเอื้อให้ธุรกิจต่างๆ บรรลุเป้าหมายเชิงกลยุทธ์ นอกจากนี้ นโยบายดังกล่าวยังมีจุดมุ่งหมายเพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูล (การรักษาความลับ การรักษาความสมบูรณ์ และการรักษาความพร้อมใช้งาน: CIA) และเพื่อให้มั่นใจว่า กลุ่ม ซีพี แอ็กซ์ตรา จะปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับทั้งหมด และให้สอดคล้องกับ กลุ่ม ซีพี (นโยบายและมาตรฐานด้านความปลอดภัยของข้อมูลของ CPG)
- นโยบายกำหนดมาตรการควบคุมที่จำเป็น และเป็นการแนะนำเกี่ยวกับการจัดเก็บ การประมวลผล และการแบ่งปันข้อมูล นอกจากนี้ยังมีรายละเอียดเกี่ยวกับความรับผิดชอบที่เกี่ยวข้องกับการปกป้องข้อมูล คุณภาพของข้อมูล การแบ่งปันข้อมูล และการกำกับดูแลข้อมูลในระดับองค์กร นโยบายจะมีมาตรฐานที่เกี่ยวข้องสนับสนุนตามความเหมาะสม
- การไม่ปฏิบัติตามนโยบายและมาตรฐาน อาจส่งผลกระทบต่อความสมบูรณ์ การกำกับดูแลข้อมูลในกลุ่ม ซีพี แอ็กซ์ตรา ส่งผลให้การตรวจสอบที่ไม่ดี ถูกแทรกแซงทางกฎหมาย ถูกปรับ มีความผิดทางอาญา เสียชื่อเสียง สูญเสีย ให้ความยินยอมของลูกค้าถูกเปิดเผย ข้อมูลที่เอื้อต่อความได้เปรียบในการแข่งขันถูกเปิดเผย และการลงโทษทางวินัยต่อพนักงาน

## 3. ขอบเขต (Scope)

นโยบายนี้ใช้กับพนักงาน ผู้รับเหมา ที่ปรึกษา พนักงานชั่วคราว ผู้ขาย และบุคคลอื่นใดที่มีส่วนร่วมในกิจกรรมเพื่อประโยชน์ของ กลุ่ม ซีพี แอ็กซ์ตรา รวมถึงบุคคลที่เกี่ยวข้องกับบุคคลที่สามซึ่งมีสิทธิ์เข้าถึงทรัพยากรข้อมูลของ กลุ่ม ซีพี แอ็กซ์ตรา

## 4. คำนิยาม (Definitions)

Term	Definition
การรักษาความลับ (Confidentiality)	ข้อมูล สารสนเทศ จะถูกเปิดเผยเฉพาะกับบุคคลที่ได้รับอนุญาตเท่านั้น
การรักษาความถูกต้อง (Integrity)	ข้อมูล สารสนเทศ มีความน่าเชื่อถือและจะแก้ไขได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น
การรักษาความพร้อมใช้ (Availability)	ข้อมูล สารสนเทศ สามารถเข้าถึงได้โดยบุคคลที่ได้รับอนุญาตเมื่อจำเป็น

Term	Definition
ผู้ใช้งานที่ได้รับอนุญาต (Authorized Users)	ผู้ใช้ที่ได้รับอนุญาต จะใช้เพื่ออ้างอิงถึงบุคคล ดังกล่าว ทั้งหมด ผู้ใช้ที่ได้รับอนุญาตต้องปฏิบัติตามนโยบายนี้ โดยถือเป็นเงื่อนไขในการใช้งานต่อเนื่องตามที่ระบุไว้ในนโยบาย

## 5. อำนาจและความรับผิดชอบในผลของงาน (Authority and Accountability)

Role	Responsibility
การควบคุม (Controls):	ธุรกิจทั้งหมดต้องดำเนินการตามขั้นตอน การควบคุมทางเทคนิค และการตรวจสอบที่เหมาะสมเพื่อให้เป็นไปตามข้อกำหนดในนโยบายและมาตรฐานสนับสนุน ผู้จัดการด้านความปลอดภัยทางไซเบอร์ต้องตรวจสอบการปฏิบัติตาม
การกำกับดูแล (Governance):	Chief Information Security Officer (CISO) มีหน้าที่ในการจัดการกับนโยบายและมาตรฐานต่าง ๆ คณะกรรมการบริษัทมีหน้าที่อนุมัตินโยบาย รวมถึงการทบทวน
การนำไปใช้งาน (Implementation):	หลังจากที่นโยบายได้รับการอนุมัติแล้ว ผู้จัดการด้านความปลอดภัยทางไซเบอร์จะสรุปกิจกรรมหลักต่าง ๆ ทั่วทั้งธุรกิจ ใน ซีพี แอ็กซ์ตรา เพื่อบูรณาการ กำกับดูแลเทคโนโลยีเข้ากับแผนการลงทุนและกิจกรรมต่อเนื่องของธุรกิจอย่างมีประสิทธิภาพ

## 6. กระบวนการด้านความเสี่ยง (Risk Methodology)

- ควรระบุความเสี่ยง เพื่อการประเมิน ปริมาณการ และจัดลำดับความสำคัญของความเสี่ยงตามเกณฑ์การยอมรับความเสี่ยงและวัตถุประสงค์ที่เกี่ยวข้องกับองค์กร ผลลัพธ์ที่ควรเป็นแนวทาง การตอบสนองความเสี่ยง และกำหนดการดำเนินการ จัดการอย่างเหมาะสมและจัดลำดับความสำคัญก่อนหลัง สำหรับการดำเนินการควบคุม และควบคุมที่เลือกมาใช้เพื่อป้องกันความเสี่ยงเหล่านี้มาใช้ อาจจำเป็นต้องดำเนินการประเมินความเสี่ยง ด้วยการเลือกการควบคุมอาจต้องดำเนินการหลายครั้งเพื่อให้ครอบคลุมส่วนต่างๆ แต่ละแอปพลิเคชันหรือระบบงานต่าง ขององค์กร
- การประเมินความเสี่ยง ควรครอบคลุมถึงแนวทางที่เป็นระบบในการประมาณขนาดของความเสี่ยง (การวิเคราะห์ความเสี่ยง) และกระบวนการเปรียบเทียบความเสี่ยงที่ประเมินไว้กับเกณฑ์ความเสี่ยง (risk map) เพื่อใช้พิจารณาความสำคัญของความเสี่ยง (การประเมินความเสี่ยง)
- ควรดำเนินการประเมินความเสี่ยงเป็นระยะ เพื่อรับมือกับการเปลี่ยนแปลงในข้อกำหนดด้านความปลอดภัยและสถานการณ์ความเสี่ยง เช่น ทรัพย์สิน ภัยคุกคาม ช่องโหว่ ผลกระทบ การประเมินความเสี่ยงและเมื่อเกิดการเปลี่ยนแปลงที่สำคัญ การประเมินความเสี่ยงเหล่านี้ควรดำเนินการในลักษณะที่มีระบบวิธีที่สามารถให้ผลลัพธ์ที่เปรียบเทียบได้และทำซ้ำได้

การประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล ควรมีขอบเขตที่ชัดเจนเพื่อให้มีประสิทธิภาพ และควรรวมความสัมพันธ์กับการประเมินความเสี่ยงในด้านอื่นๆ ด้วย กรุณาอ้างอิง มาตรฐานการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย (Information Security Risk Management Standard)

## 7. การจัดองค์กร ด้านการรักษาความมั่นคงปลอดภัย (Organization of Information Security)

### 7.1 การจัดองค์กรภายใน (Internal Organization)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องกำหนดกรอบการจัดการเพื่อริเริ่ม ควบคุมการนำไปปฏิบัติ และการดำเนินงานด้านความปลอดภัยของข้อมูลภายในองค์กร

#### 7.1.1 การให้คำมั่นของผู้บริหารในเรื่องการรักษาความมั่นคง (Management Commitment to Information Security)

ผู้บริหารจะต้องสนับสนุน การรักษาความมั่นคงปลอดภัยภายในองค์กรอย่างเข้มแข็ง ด้วยการให้ผ่านทิศทางที่ชัดเจน มุ่งมั่นที่แสดงให้เห็น การมอบหมายบุคลากร ที่ชัดเจน และ การรับรู้หน้าที่ด้านความปลอดภัยของข้อมูล

#### 7.1.2 การประสานงานด้านการรักษาความมั่นคงปลอดภัย (Information Security Coordination)

ทีมงานด้านความปลอดภัยของข้อมูลของ กลุ่ม ซีพี แอ็กซ์ตรา ให้คำแนะนำ แนวทาง และอำนาจในการดำเนินกิจกรรมด้านการรักษาความปลอดภัยของข้อมูล ทีมจะดำเนินการประเมินการปฏิบัติตามอย่างสม่ำเสมอทั้งจากภายในและจากภายนอกเป็นประจำ ทั้งหมดของ กลุ่ม ซีพี แอ็กซ์ตรา เพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดด้านการรักษาความปลอดภัยของข้อมูล

#### 7.1.3 หน้าที่และความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย (Information Security Roles and Responsibilities)

ความรับผิดชอบด้านการรักษาความปลอดภัยของข้อมูล ทั้งหมดจะถูกกำหนดและจัดสรร

##### 1) การบริหารด้านการ รักษาความมั่นคงปลอดภัย Information Security Management

- ทำให้มั่นใจว่า เป้าหมายด้านการรักษาความปลอดภัยของข้อมูลได้รับการกำหนด การปฏิบัติ ตามสอดคล้องกับความต้องการขององค์กร และมีการบูรณาการเข้าไปในกระบวนการทำงาน ที่เกี่ยวข้อง
- ให้ทิศทางที่ชัดเจนและสนับสนุนการจัดการในเรื่อง การรักษาความมั่นคงปลอดภัย
- จัดเตรียมทรัพยากรที่จำเป็นสำหรับ การรักษาความปลอดภัยข้อมูล
- จัดให้มี การทบทวนนโยบาย การรักษาความปลอดภัยข้อมูล เป็นประจำทุกปี

##### 2) ความรับผิดชอบด้านความปลอดภัยต้องกำหนด ถึงก่อนการจ้างงาน ในรายละเอียดงานที่เหมาะสม และเงื่อนไขและข้อกำหนดในการจ้างงาน

##### 3) ผู้บริหารต้อง ดำเนินการฝึกอบรมเกี่ยวกับการปฏิบัติตามกฎเกณฑ์ เพื่อให้มั่นใจว่าทุกคน ผู้ใช้งาน หรือที่เข้าถึงทรัพยากรสารสนเทศ เข้าใจหน้าที่และความรับผิดชอบของตนเอง โดยจะต้องมีการจัดการฝึกอบรมก่อนที่จะได้รับอนุญาตให้เข้าถึงทรัพยากรข้อมูล

##### 4) บทบาทและความรับผิดชอบด้านการรักษาความปลอดภัยสำหรับพนักงาน ผู้รับเหมา และบุคคลภายนอก มีดังต่อไปนี้:

- แต่ละคนต้องปฏิบัติตามนโยบายการรักษาความปลอดภัยข้อมูลขององค์กร
  - แต่ละคนจะต้องกระทำเพื่อปกป้องทรัพย์สิน จากการเข้าถึง การเปิดเผย การแก้ไข ดัดแปลง การทำลาย หรือหรือการแทรกแซงโดยไม่ได้รับอนุญาต
  - แต่ละคนต้องดำเนินการตามกระบวนการหรือกิจกรรมด้านการรักษาความปลอดภัย ให้สอดคล้องกับหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย
  - แต่ละคนจะต้องทำอย่างโปร่งใส และรับผิดชอบต่อผลของการกระทำที่เกิดขึ้น
  - แต่ละคนจะต้องทราบถึงวิธีการและการแจ้งเหตุการณ์ หรือเหตุการณ์หรือความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้น
- 5) สำหรับบุคคลที่สาม บทบาทด้านความปลอดภัยและความรับผิดชอบจะต้องรวมอยู่ในคำชี้แจงการทำงาน (statement of work) ข้อตกลงระดับการให้บริการ และ/หรือสัญญา
- 6) การปกป้องข้อมูลจะต้องรวมอยู่ในคำอธิบายงานและหน้าที่ เป้าหมายและวัตถุประสงค์ประจำปี การประเมินผลการปฏิบัติงาน ตารางคะแนนส่วนบุคคล และคำตอบแทน

#### 7.1.4 การติดต่อกับเจ้าหน้าที่ทางการ (Contact with Authorities)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมีการปฏิบัติงานในตามที่กำหนดไว้ว่าจะต้องติดต่อใครและเมื่อใดในเวลาที่เหมาะสม หากมีการละเมิดกฎหมายหรือเกิดเหตุการณ์ผิดปกติที่รุนแรงเกิดขึ้น มีผลกระทบต่อสิทธิของลูกค้ำ

#### 7.1.5 การติดต่อกับกลุ่มเฉพาะทาง (Contact with Special Interest Groups)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมีข้อมูลการติดต่อกับกลุ่มเฉพาะทาง หรือฟอรัมด้านการรักษาความปลอดภัยเฉพาะทาง หรือ ฟอรัมด้านการรักษาความมั่นคงปลอดภัย หรือสมาคมวิชาชีพ เพื่อติดตามความเสี่ยงใหม่ ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การสอบทานการแจ้งเตือนและข้อเสนอแนะด้านการรักษาความมั่นคงปลอดภัยสารสนเทศจากเจ้าของผลิตภัณฑ์ หรือกลุ่มอุตสาหกรรม เป็นสิ่งที่ควรดำเนินการ

#### 7.1.6 การรักษาความมั่นคงปลอดภัยสารสนเทศ ในการบริหารโครงการ (Information security in project management)

จำเป็นต้องมีการตรวจสอบโปรแกรมรักษาความปลอดภัยข้อมูลของกลุ่ม ซีพี แอ็กซ์ตรา อย่างเป็นอิสระตามช่วงเวลาที่กำหนดหรือเมื่อเกิดการเปลี่ยนแปลงที่สำคัญในการดำเนินการรักษาความปลอดภัย ผลลัพธ์ จะได้รับการบันทึกและเก็บรักษาไว้

#### 7.1.7 เราจะติดตามการรักษาความปลอดภัยของข้อมูลโดยอิสระ (Independent Review of Information security)

จำเป็นต้องมีการทบทวนโปรแกรมรักษาความปลอดภัยข้อมูลของกลุ่ม ซีพี แอ็กซ์ตรา อย่างเป็นอิสระตามช่วงเวลาที่กำหนด (อย่างน้อยปีละครั้งหรือเมื่อเกิดการเปลี่ยนแปลงที่สำคัญในการดำเนินการรักษาความปลอดภัย) ผลลัพธ์ จะได้รับการบันทึกและรักษาไว้

## 7.2 ส่วนงานภายนอก (External Parties)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องรักษาไว้ซึ่งทรัพยากรสารสนเทศและทรัพยากรคอมพิวเตอร์ของการประมวลผลขององค์กรที่ถูกรับเข้าถึง ประมวลผล สื่อสาร จัดการโดยส่วนงานภายนอก โดยอ้างอิง มาตรฐานความปลอดภัยความสัมพันธ์กับผู้ขาย (Information Security in Supply Chain Standard)

## 8. การรักษาความมั่นคงปลอดภัยทรัพยากรบุคคล (Human Resource Security)

### 8.1 ก่อนการว่าจ้าง (Prior Employment)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องให้มั่นใจว่าพนักงาน และผู้รับเหมาของกลุ่ม ซีพี แอ็กซ์ตรา ต้องมีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย และลดความเสี่ยงจากการขโมย ทูจริต หรือใช้ทรัพย์สินอุปกรณ์โดยมิชอบ

### 8.2 ระหว่างการว่าจ้าง (During Employment)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องให้มั่นใจว่าพนักงานทั้งหมด ตระหนักถึงภัยคุกคามและข้อกังวลด้านความปลอดภัยของข้อมูล ตลอดจนความรับผิดชอบและภาระผูกพันของตน และพร้อมที่จะสนับสนุนนโยบายการรักษาความปลอดภัยขององค์กรในระหว่างการทำงานปกติ และลดความเสี่ยงจากข้อผิดพลาดส่วนบุคคล

### 8.3 หลังสิ้นสุดการว่าจ้าง (Post Employment)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องปกป้องผลประโยชน์ขององค์กร ซึ่งเป็นส่วนหนึ่งของการเปลี่ยนแปลง หรือการเลิกจ้าง โดยอ้างอิง มาตรฐานความปลอดภัยทรัพยากรบุคคล (Human Resource Security Standard).

## 9. การจัดการทรัพย์สิน (Asset management)

### 9.1 หน้าที่ในการจัดการทรัพย์สิน (Responsibility for Assets)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องระบุทรัพย์สินขององค์กรและกำหนดความรับผิดชอบในการป้องกันที่เหมาะสม ทรัพย์สินข้อมูลสารสนเทศสำคัญทั้งหมดจะต้องได้รับการระบุอย่างชัดเจน ข้อมูล โดยอ้างอิง มาตรฐานการจัดการสินทรัพย์ไอที (IT Asset Management Standard)

### 9.2 การจัดประเภทสารสนเทศ (Information Classification)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องให้มั่นใจว่าข้อมูลสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามความสำคัญต่อองค์กร ข้อมูลสารสนเทศจะต้องได้รับการจำแนกประเภทตามข้อกำหนดทางกฎหมาย มูลค่า ความสำคัญ และความอ่อนไหวต่อการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

### 9.3 การดูแลสื่อ (Media Handling)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการเปิดเผย การแก้ไข การลบ หรือการทำลายทรัพย์สินที่ไม่ได้รับอนุญาต รวมถึงการหยุดชะงักของกิจกรรมทางธุรกิจ กรุณาอ้างอิง มาตรฐานการจัดการสินทรัพย์ไอที (IT Asset Management Standard)

## 10. การควบคุมการเข้าถึง (Access control)

### 10.1 การร้องเรียนเกี่ยวกับเรื่องนี้เป็นทางการ (Business requirement of access control)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องจำกัดการเข้าถึงข้อมูลสารสนเทศ สถานที่อุปกรณ์ในการประมวลผลสารสนเทศ นโยบายการควบคุมการเข้าถึงจะต้องได้รับการจัดทำเป็นเอกสารและทบทวนตามข้อกำหนดด้านการรักษาความปลอดภัยของธุรกิจและข้อมูล กรุณาอ้างอิง มาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management Standard)

### 10.2 การจัดการการเข้าถึง (User access management)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบและบริการได้ โดยไม่ได้ขั้นตอนการปฏิบัติที่เป็นทางการต้องถูกกำหนดเพื่อควบคุมการให้สิทธิในการเข้าถึงทรัพยากรประมวลผลและบริการ ขั้นตอนการปฏิบัติงานต้องครอบคลุมตั้งแต่สร้างผู้ใช้งานใหม่ในระบบจนถึงลบออกจากระบบเมื่อหมดความจำเป็น กรุณาอ้างอิง มาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management Standard)

### 10.3 หน้าที่ของผู้ใช้ (User responsibilities)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการเข้าถึงของผู้ใช้ที่ไม่ได้รับอนุญาต รวมถึงการบุกรุกหรือการขโมยทรัพยากรสารสนเทศ และทรัพยากรประมวลผล พนักงานของกลุ่ม ซีพี แอ็กซ์ตรา ต้องปฏิบัติตาม มาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง และมาตรฐานจัดการรหัสผ่าน (Identity and Access Management Standard and Password Management Standard)

### 10.4 การควบคุมการเข้าถึงระบบและระบบงาน (System and application access control)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการเข้าถึงระบบงานและแอปพลิเคชันโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลสารสนเทศและระบบแอปพลิเคชันของพนักงานกลุ่ม ซีพี แอ็กซ์ตรา ต้องถูกจำกัดตาม มาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง และมาตรฐานจัดการรหัสผ่าน (Identity and Access Management Standard and Password Management Standard)

## 11. การเข้ารหัส (Cryptography)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องปกป้องการรักษาความลับ ความถูกต้อง หรือ ความถูกต้องของสารสนเทศด้วยวิธีการเข้ารหัส

### 11.1 การควบคุมการเข้ารหัส (Cryptographic controls)

การเข้ารหัสเพื่อปกป้องข้อมูลลับของกลุ่ม ซีพี แอ็กซ์ตรา ระดับการป้องกันที่กำหนดไว้ใน มาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง และมาตรฐานการจัดการการเข้ารหัสและการจัดการคีย์ (Identity and Access Management Standard and Cryptography and Key Management Standard)

## 12. การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environment security)

### 12.1 พื้นที่รักษาความปลอดภัย (Secure areas)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการเข้าถึงทางกายภาพที่ไม่ได้รับอนุญาต ป้องกันจากการทำลาย หรือแทรกแซง ทรัพย์สิน และบริการในพื้นที่ขององค์กร การรักษาความมั่นคงปลอดภัยพื้นที่อาณาเขต เช่น ประตู กำแพง ควรนำมาใช้ปกป้องบริเวณพื้นที่ ที่เก็บทรัพยากรสารสนเทศและทรัพยากรประมวลผล กรุณาอ้างอิง มาตรฐานการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security Standard)

### 12.2 อุปกรณ์ (Equipment)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องปกป้องทรัพย์สินจากการสูญหาย เสียหาย ถูกขโมย ถูกละเมิด หรือทำให้หยุดชะงักต่อการปฏิบัติงานของบริษัท กลุ่ม ซีพี แอ็กซ์ตรา อุปกรณ์ทั้งหมดที่จำเป็นสำหรับการปฏิบัติงานของกลุ่ม ซีพี แอ็กซ์ตรา (การประมวลผล การสื่อสาร การจัดเก็บข้อมูล) จะต้องได้รับการปกป้องอย่างเหมาะสมจากภัยคุกคามต่อสิ่งแวดล้อมในพื้นที่ กรุณาอ้างอิง มาตรฐานการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security Standard)

## 13. การรักษาความมั่นคงปลอดภัยด้านการปฏิบัติการ (Operations security)

### 13.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบด้านการปฏิบัติการ (Operational procedures and responsibilities)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องดำเนินการให้มั่นใจว่าระบบประมวลผลข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย ขั้นตอนการปฏิบัติงานอย่างเป็นทางการจะต้องได้รับการออกแบบ จัดทำเป็นลายลักษณ์อักษร และบำรุงรักษาสำหรับนำไปปฏิบัติ สำหรับการปฏิบัติงานประจำวันทรัพยากรคอมพิวเตอร์ทั้งหมดที่จัดเก็บ ประมวลผล หรือส่งข้อมูลของกลุ่ม ซีพี แอ็กซ์ตรา เอกสารจะต้องได้รับการเผยแพร่และเปิดให้พนักงานของกลุ่มบริษัท ซีพี แอ็กซ์ตรา ที่มีหน้าที่รับผิดชอบด้านปฏิบัติการด้านไอทีทุกคนเข้าถึงได้ง่าย กรุณาอ้างอิง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านการปฏิบัติงาน (Operations Security Standard)

### 13.2 การป้องกันโปรแกรมประสงค์ร้าย (Protection from Malware)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องให้มั่นใจว่าข้อมูลสารสนเทศและสถานที่อุปกรณ์สำหรับในการประมวลผลข้อมูลได้รับการปกป้องโปรแกรมจากมัลแวร์ ระบบทั้งหมดที่มักได้รับผลกระทบทั้งเว็รกสเตชันและเซิร์ฟเวอร์จะต้องใช้ซอฟต์แวร์ป้องกันไวรัสที่ได้รับการจัดการจากส่วนกลางที่ได้รับการอนุมัติ ผู้ใช้ไม่ได้รับอนุญาตให้ปิดใช้งานระบบ ช้าม หรือเปลี่ยนแปลงสถานะของซอฟต์แวร์ป้องกันไวรัสเพื่อลดประสิทธิภาพ กรุณาอ้างอิง มาตรฐานการรักษาความมั่นคงปลอดภัยด้านการปฏิบัติงาน (Operations Security Standard)



### 13.3 การสำรองข้อมูล (Backup)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการสูญเสียด้านข้อมูล การสำเนาข้อมูลและซอฟต์แวร์ ต้องทำและทดสอบอย่างสม่ำเสมอ ตามนโยบายสำรองข้อมูลที่ตกลงร่วมกัน ระดับของสำรองข้อมูล ถึงกำหนดไว้ใน มาตรฐานการรักษาความปลอดภัยด้านการปฏิบัติงาน (Operations Security Standard)

### 13.4 การเก็บข้อมูลจราจรคอมพิวเตอร์ (Logging and monitoring)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องบันทึกเหตุการณ์และเก็บหลักฐานเหตุการณ์ ข้อกำหนดความต้องการสำหรับการเก็บข้อมูลจราจรทางคอมพิวเตอร์ การเฝ้าติดตามข้อมูลจราจรทางคอมพิวเตอร์ การเทียบเวลามาตรฐานระยะเวลาในการเก็บข้อมูลจราจรคอมพิวเตอร์ด้านการรักษาความมั่นคงปลอดภัย และการปกป้องข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บ สามารถดูได้จาก มาตรฐานการเฝ้าติดตามข้อมูลจราจรคอมพิวเตอร์ (Log Monitoring Standard)

### 13.5 การควบคุมซอฟต์แวร์ปฏิบัติการ (Control of operational software)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าระบบปฏิบัติการมีความถูกต้องสมบูรณ์ การติดตั้งและอัปเดตซอฟต์แวร์ทั้งหมดบนระบบที่บริหารจัดการจากส่วนกลางควรดำเนินการตามกระบวนการจัดการการเปลี่ยนแปลงของกลุ่ม ซีพี แอ็กซ์ตรา กรุณาอ้างอิง มาตรฐานการรักษาความปลอดภัยด้านการปฏิบัติงาน (Operations Security Standard)

### 13.6 การจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค การประเมินช่องโหว่และค่าพื้นฐานระบบ (Baseline) รายละเอียดใน มาตรฐานการจัดการช่องโหว่ (Vulnerability Management Standard) และกรอบดำเนินงานด้านการทดสอบเจาะระบบ (Penetration testing framework)

### 13.7 สิ่งที่ต้องพิจารณาในการตรวจระบบสารสนเทศ (Information systems audits considerations)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องลดผลกระทบของกิจกรรมการตรวจสอบต่อระบบปฏิบัติ การให้เหลือน้อยที่สุด การเข้าถึงเครื่องมือตรวจสอบระบบสารสนเทศจะต้องได้รับการปกป้องเพื่อป้องกันการใช้งานในทางที่ผิดหรือการละเมิด ที่อาจเกิดขึ้นได้ กรุณาอ้างอิง มาตรฐานการรักษาความปลอดภัยด้านการปฏิบัติงาน (Operations Security Standard)

## 14. การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร (Communication Security)

### 14.1 การจัดการการรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security management)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าการปกป้องข้อมูลในเครือข่ายและอุปกรณ์ประมวลผลข้อมูลการสนับสนุนระดับการป้องกันสารสนเทศในเครือข่าย กำหนดไว้ใน มาตรฐานการรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security Standard)

### 14.2 การส่งสารสนเทศ (Information transfer)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องดูแลรักษาความปลอดภัยของข้อมูลที่ถ่ายโอนภายในองค์กรและกับหน่วยงานภายนอก ระดับที่จำเป็นในการถ่ายโอนข้อมูลนั้นกำหนดไว้ใน มาตรฐานการรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security Standard)

## 15. การจัดหา การพัฒนา และการดูแลระบบ (System acquisition, development, and maintenance)

### 15.1 ข้อกำหนดความต้องการด้านการรักษาความมั่นคงปลอดภัย สำหรับระบบสารสนเทศ (Security requirements of information systems)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าการรักษาความปลอดภัยของข้อมูลสารสนเทศได้บูรณาการเข้าไปเป็นส่วนหนึ่งของระบบสารสนเทศระบบสารสนเทศตลอดทั้งวงจรชีวิต ที่ให้บริการผ่านเครือข่ายสาธารณะด้วย การออกแบบระบบและแอปพลิเคชันทั้งหมดควรต้องปฏิบัติตาม มาตรฐานวัฏจักรการพัฒนาแบบอย่างปลอดภัย (Secure Software Development Life Cycle Standard)

### 15.2 การรักษาความมั่นคงปลอดภัยสารสนเทศในกระบวนการพัฒนาและการ (Security in development and support processes)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าการรักษาความปลอดภัยของข้อมูลสารสนเทศ ได้รับการออกแบบและนำไปใช้ภายในวงจรชีวิตการพัฒนาระบบสารสนเทศ กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบควรได้รับการกำหนดและนำไปใช้กับการพัฒนาภายใน กลุ่ม ซีพี แอ็กซ์ตรา อ้างอิง มาตรฐานวัฏจักรการพัฒนาแบบอย่างปลอดภัย (Secure Software Development Life Cycle Standard)

### 15.3 ข้อมูลทดสอบ (Test data)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าข้อมูลการทดสอบจะต้องได้รับการปกป้องและควบคุม ข้อมูลสภาพแวดล้อมการใช้งานจริงที่นำมาใช้ในสภาพแวดล้อมการทดสอบต้องถูก(ไม่ระบุชื่อ) เพื่อปกป้องความลับของข้อมูล สามารถดูข้อมูลเพิ่มเติมได้ใน มาตรฐานการจำแนกประเภทข้อมูลและการจัดการ (Information Classification and Handling Standard)

## 16. ความสัมพันธ์กับผู้ขาย (Supplier relationships)

### 16.1 การรักษาความมั่นคงปลอดภัยในด้านความสัมพันธ์กับผู้ขาย (Information security in supplier relationships)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่ามีการปกป้องทรัพย์สินขององค์กรที่ผู้ขายสามารถ เข้าถึงได้ ข้อกำหนดด้านความปลอดภัยของข้อมูลสำหรับลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงของผู้ขาย ควรได้รับการตกลงและทำเป็นลายลักษณ์อักษร ข้อกำหนดด้านความปลอดภัยของข้อมูลที่เกี่ยวข้องทั้งหมดควรได้รับการจัดทำและตกลงกับผู้ขาย แต่ละรายที่อาจเข้าถึง ประมวลผล จัดเก็บ สื่อสาร หรือจัดหาโครงสร้างพื้นฐานไอทีสำหรับองค์กร กรุณาอ้างอิง มาตรฐานความปลอดภัยความสัมพันธ์กับผู้ขาย (Information Security in Supply Chain Standard)

### 16.2 การจัดการการส่งมอบบริการของผู้ขาย (Supplier service delivery management)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องดูแลระดับการรักษาความปลอดภัยของข้อมูลและการส่งมอบบริการที่ตกลงกันไว้ตามข้อตกลงกับผู้ขาย สัญญาอย่างเป็นทางการจะต้องมีอยู่กับผู้ให้บริการบุคคลที่สามทั้งหมดสำหรับ กลุ่ม ซีพี แอ็กซ์ตรา สัญญาเหล่านี้จะต้องกำหนดระดับการบริการและข้อตกลงการส่งมอบที่ตกลงกันไว้ และต้องระบุถึงการติดตามผลการปฏิบัติงานอย่างต่อเนื่องเทียบกับข้อผูกพันเหล่านี้ สัญญาเหล่านี้ควรทำขึ้นหลังจากดำเนินการตรวจสอบความครบถ้วนถูกต้องที่เหมาะสมสำเร็จแล้วเท่านั้น สัญญาของบุคคลที่สามทั้งหมดจะต้องระบุว่าผู้ให้บริการแก่ กลุ่ม ซีพี แอ็กซ์ตรา จะต้องผูกพันตามนโยบายและมาตรฐานของ กลุ่ม ซีพี แอ็กซ์ตรา สัญญาเหล่านี้ควรระบุถึงสิทธิ์ของ กลุ่ม ซีพี แอ็กซ์ตรา ที่จะทำการตรวจสอบผลการปฏิบัติงานเป็นประจำเทียบกับระดับการบริการที่ตกลงกันไว้และการปฏิบัติตามข้อกำหนดของ กลุ่ม ซีพี แอ็กซ์ตรา กรุณาอ้างอิง มาตรฐานความปลอดภัยความสัมพันธ์กับผู้ขาย (Information Security in Supply Chain Standard)

## 17. การจัดการเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัย (Information security incident management)

### 17.1 การจัดการเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยและการปรับปรุง (Management of information security incidents and improvements)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าเหตุการณ์ด้านการรักษาความปลอดภัยของข้อมูลและจุดอ่อนที่เกี่ยวข้องกับระบบสารสนเทศต้องได้รับการสื่อสารให้สามารถดำเนินการแก้ไขได้ทันที่ข้อกำหนดดังกล่าวได้กำหนดไว้ใน มาตรฐานการจัดการเหตุการณ์ผิดปกติด้านการรักษาความปลอดภัย (Security Incident Management Standard)

## 18. การจัดการความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

### 18.1 ความต่อเนื่องของการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

ความต่อเนื่องด้านการรักษาความปลอดภัยของข้อมูล ต้องฝังไว้ในระบบการจัดการความต่อเนื่องทางธุรกิจขององค์กร (Organization's business continuity management systems)

#### 18.1.1 การวางแผนความต่อเนื่องของการรักษาความมั่นคงของ (Planning Information Security continuity)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องกำหนดข้อกำหนดด้านการรักษาความปลอดภัยของข้อมูลและความต่อเนื่องของการจัดการด้านความปลอดภัยของข้อมูลในสถานการณ์ที่ไม่เอื้ออำนวย เช่น ในช่วงวิกฤตการณ์หรือภัยพิบัติ

#### 18.1.2 การนำความต่อเนื่องของการรักษาความมั่นคงปลอดภัยไปใช้ (Implementing information security continuity)

กลุ่ม ซีพี แอ็กซ์ตรา จะต้องจัดทำ จัดทำเอกสาร นำไปปฏิบัติ และบำรุงรักษากระบวนการ ขั้นตอน และการควบคุมเพื่อให้มั่นใจถึงระดับความต่อเนื่องที่จำเป็นสำหรับการรักษาความปลอดภัยของข้อมูลในสถานการณ์ที่ไม่เอื้ออำนวย

#### 18.1.3 ตรวจสอบ สอบทาน และประเมินความต่อเนื่องของการรักษาความมั่นคงปลอดภัย (Verify, review, and evaluate information security continuity)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องตรวจสอบการควบคุมความต่อเนื่องของการรักษาความปลอดภัยของข้อมูลที่จัดทำและนำไปปฏิบัติเป็นระยะๆ เพื่อให้แน่ใจว่าการควบคุมดังกล่าวถูกต้องและมีประสิทธิภาพในสถานการณ์ที่ไม่พึงประสงค์

### 18.2 การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าสิ่งอุปกรณ์อำนวยความสะดวกในการประมวลผลข้อมูลพร้อมใช้งาน อุปกรณ์ประมวลผลสารสนเทศ ต้องมีการเตรียมสำรองไว้เพียงพอ เพื่อให้ตรงกับข้อกำหนดความต้องการเรื่องความพร้อมใช้

## 19. การปฏิบัติตาม (Compliance)

### 19.1 การปฏิบัติตามข้อกำหนดความต้องการทางกฎหมายและสัญญา (Compliance with legal and contractual requirements)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องหลีกเลี่ยงการละเมิดกฎหมาย กฎระเบียบ หรือข้อผูกพันตามสัญญาใดๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและข้อกำหนดใดๆ กรุณาอ้างอิง มาตรฐานการปฏิบัติตาม (Compliance Standard)

### 19.2 การสอบทานการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

กลุ่ม ซีพี แอ็กซ์ตรา ต้องมั่นใจว่าการรักษาความปลอดภัยข้อมูลได้รับการดำเนินการงานตามนโยบายและขั้นตอนขององค์กร

## 20. ข้อยกเว้น (Exceptions)

เจ้าของหน่วยธุรกิจต้องปฏิบัติตาม นโยบายความปลอดภัยของข้อมูล Information Security Policy (ISP) ในกรณีเจ้าของหน่วยธุรกิจไม่สามารถปฏิบัติตามนโยบายและมาตรฐานนี้ได้ เจ้าของหน่วยธุรกิจต้องได้รับการอนุมัติจากคณะกรรมการบริหารเทคโนโลยีสารสนเทศ และความปลอดภัย สำหรับข้อยกเว้นใดๆ เจ้าของธุรกิจที่เกี่ยวข้องต้องแสดงหลักฐานและเหตุผลต่อ คณะกรรมการบริหารเทคโนโลยีสารสนเทศ และความปลอดภัย เพื่อแสดงให้เห็นถึงความจำเป็นทางธุรกิจและข้อจำกัดของตนตาม นโยบายความปลอดภัยของข้อมูล Information Security Policy (ISP)

## 21. บทลงโทษ (Penalties)

พนักงานทุกคนต้องให้ความร่วมมืออย่างเต็มที่กับหน่วยงานภายในและภายนอกในกรณีที่เกิดการสอบสวน การละเมิดหรือการไม่ปฏิบัติตามนโยบายและมาตรฐานนี้ทั้งทางตรงและทางอ้อม โดยฝ่ายบริหารและพนักงานจะต้องได้รับการลงโทษทางวินัยตามระเบียบข้อบังคับของบริษัท

## 22. อ้างอิง (References)

- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- CPG Information Security Policy & Standards (English) – 15 July 2021