2. ความรับผิดชอบต่อความมั่นคงปลอดภัยสารสนเทศ

2.1 ผู้ใช้ต้องทำความเข้าใจ และปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศที่กำหนด

2.2 ผู้ใช้ต้องปรึกษากับผู้จัดการตามสายบังคับบัญชา หรือ หน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อคลายข้อสงสัยใด ๆ เกี่ยวข้องนโยบายเหล่านั้น

2.3 ผู้ใช้ต้องรายงานเรื่องดังต่อไปนี้แก่ผู้บริหารตามสายบังคับบัญชา หรือ หน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ

ก) เหตุการณ์ที่น่าสงสัย หรือ เหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข) จุดอ่อนด้านการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับคน กระบวนการ และ/หรือ ระบบ

ค) ความเสี่ยงทางด้านการรักษาความมั่นคงปลอดภัย และ/หรือ

ง) ประเด็นปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัย

2.4 ผู้ใช้ต้องไม่ละเมิดการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่บริษัทจัดทำขึ้น

2.5 ผู้ใช้ต้องปฏิบัติตามสัญญาการไม่เปิดเผยข้อมูล (NDA) ตลอดเวลาการเป็นพนักงาน, การว่าจ้าง ตลอดจนหลังจากสัญญาว่าจ้างสิ้นสุด

2.6 ผู้ใช้ต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล และนโยบายการรักษาความปลอดภัยข้อมูลของบริษัท ในกรณีข้อมูลส่วนบุคคลรั่วไหล หรือข้อมูลความลับของบริษัทรั่วไหล ผู้ใช้ เจ้าของข้อมูล หรือเจ้าของระบบ ต้องแจ้งฝ่ายคุ้มครองข้อมูลส่วนบุคคล และหน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ โดยทันที

3. การใช้งานทรัพย์สิน

3.1 ผู้ใช้มีหน้าที่รับผิดชอบดังต่อไปนี้

การใช้ระบบ และ เครือข่าย

- ห้ามนำโปรแกรมประสงค์ร้าย (malicious programs) เข้าสู่เครือข่ายหรือเครื่องแม่ข่าย (เช่น ไวรัส เวิร์ม ไวรัสม้าโทรจัน อีเมลบอมบ์ ฯลฯ)
- ห้ามเปิดเผยรหัสผ่านแก่ผู้อื่น หรือ อนุญาตให้บุคคลอื่นใช้บัญชีผู้ใช้งานของตนเอง
- ห้ามละเมิดมาตรการด้านความปลอดภัย หรือ การทำให้เครือข่ายการติดต่อสื่อสารหยุดชะงัก
- ห้ามทำสแกนพอร์ท (Port Scanning) หรือ การสแกนด้านการรักษาความมั่นคงปลอดภัย ยกเว้นกระทำโดยพนักงานหรือคู่สัญญาที่ได้รับอนุญาต
- ห้ามดักจับข้อมูลในระบบเครือข่าย ยกเว้นการกระทำนั้นเป็นส่วนหนึ่งของหน้าที่ปกติของพนักงานนั้น ๆ
- ห้ามหลีกเลี่ยงการพิสูจน์ตัวตนหรือมาตรการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย, เครือข่าย หรือระบบงาน
- ห้ามโจมตีเครื่องคอมพิวเตอร์หรือเครือข่ายอื่น ๆ เช่น การโจมตีให้เกิดการหยุดชะงักในการให้บริการ (Denial of service attack)
- ห้ามรบกวน หรือทำให้การใช้งานเซสชันของผู้ใช้หยุดชะงัก
- ห้ามเปิดเผยข้อมูลเกี่ยวกับพนักงาน หรือ ลิสต์รายชื่อพนักงานแก่บุคคลภายนอก
- ห้ามเปิดเผยข้อมูลระบบ หรือ มาตรการป้องกันด้านการรักษาความมั่นคงปลอดภัยของกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า แก่บุคคลที่ไม่ได้รับอนุญาต

การเข้าถึงระบบงานจากทางไกล (Remote access)

- สิทธิในการเข้าถึงจากทางไกลจะให้เมื่อจำเป็น และระงับทันทีเมื่อ เมื่อลาออก, สิ้นสุดความจำเป็นในการใช้งาน, สิ้นสุดโครงการ
- การเข้าถึงจากทางไกลไม่ว่าจะเป็น VPN, SSH ฯลฯ เพื่อเข้ามาดำเนินงานเสมือนดำเนินการในพื้นที่ทำงานปกติ ต้องได้รับการอนุมัติจากหน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ และต้องได้รับการต่ออายุทุก 3 เดือน
- ห้ามใช้ Service การเชื่อมต่อทางไกล นอกเหนือจากที่ทาง IT จัดหาให้
- ห้ามให้ผู้อื่นเข้าถึงหรือใช้เครื่องคอมพิวเตอร์ระหว่างที่มีการเชื่อมต่อจากทางไกล

การใช้งานคอมพิวเตอร์

- ผู้ใช้ต้องดูแลเรื่องการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ และ จำกัดการเข้าถึงเครื่องคอมพิวเตอร์เดสก์ท็อป ทั้งทางกายภาพ และทางตรรกะ (logical access)
- ห้ามเปลี่ยนค่าระบบของฮาร์ดแวร์ การตั้งค่าในระบบปฏิบัติการ หรือ ระบบงานที่ติดตั้งบนเครื่องคอมพิวเตอร์เดสก์ท็อป หากผู้ใช้ต้องการการเปลี่ยนแปลงใด ๆ ให้ติดต่อผู้บังคับบัญชา และขออนุมัติพร้อมเหตุผลในการดำเนินการดังกล่าว
- การใช้งานของบัญชีที่มีสิทธิสูง (administrative rights) ของทุกระบบจะปิดไม่ให้ใช้งาน หากมีความประสงค์ที่ต้องใช้งานสิทธิดังกล่าว ต้องขออนุมัติพร้อมเหตุผลจากผู้บังคับบัญชา
- ห้ามมิให้ผู้ใช้ทำให้เกิดการเข้าถึงจากเครือข่ายภายนอกโดยตรง เช่น ผ่านการเชื่อมต่อผ่าน VPN ส่วนบุคคล ผ่านการปล่อยสัญญาณโทรศัพท์มือถือ

เพื่อป้องกันความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต ผู้ใช้ควรปฏิบัติมาตรการต่อไปนี้:

- ให้ออกจากระบบงานทั้งหมด หรือ ปิดเครื่องคอมพิวเตอร์เดสก์ท็อป หากต้องทิ้งเครื่องคอมพิวเตอร์เดสก์ท็อปไว้โดยไม่มีใครดูแลเป็นระยะเวลานาน
- ให้เปิดใช้โปรแกรมรักษาหน้าจอ (screen saver) ที่มีรหัสผ่าน หากต้องทิ้งเครื่องคอมพิวเตอร์เดสก์ท็อปเป็นระยะเวลาสั้น ๆ
- ห้ามแชร์โฟลเดอร์ในคอมพิวเตอร์กับผู้ใดผ่านเครือข่าย

การใช้งานอินเทอร์เน็ต

- ผู้ใช้ควรเข้าถึงอินเทอร์เน็ตเพื่อจุดประสงค์ทางธุรกิจ
- การใช้อินเทอร์เน็ตในเรื่องส่วนตัวเป็นครั้งคราวตามสมควรสามารถทำได้ โดยที่ต้องไม่มีผลกระทบต่อประสิทธิภาพการทำงาน
- ผู้ใช้จะต้องทำการพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ต และให้เข้าถึงเฉพาะเว็บไซต์ที่เกี่ยวข้องกับการทำงาน กลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า จะมีสิทธิ์ในการกรอง และห้ามการเข้าถึงบางเว็บไซต์
- ห้ามผู้ใช้ใช้อินเทอร์เน็ตในการกระทำ ดังนี้
    - ดาวน์โหลด หรือส่งต่อซอฟต์แวร์ประสงค์ร้ายหรือแพร่กระจายไวรัส
    - ละเมิดข้อตกลงด้านลิขสิทธิ์
    - อัปโหลดไฟล์ซอฟต์แวร์ หรือข้อมูลของกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า ไปยังเว็บไซต์อินเทอร์เน็ตใด ๆ โดยไม่ได้รับอนุญาต
    - เปิดเผยข้อมูลที่เป็นความลับ หรือ ข้อมูลที่ละเอียดอ่อนของกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า โดยไม่ได้รับอนุญาต
    - โพสต์มุมมอง หรือ ความคิดเห็นในนามของกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า โดยไม่ได้รับอนุญาต
    - เข้าเว็บไซต์ ที่ผิดกฎหมาย หรือ จริยธรรม เช่น การพนัน ภาพลามกอนาจาร

การใช้อีเมล

- ห้ามมิให้ส่งหรือส่งต่ออีเมลที่มีข้อมูลอันเป็นความลับของกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า ได้แก่ ข้อมูลลูกค้า กลยุทธ์ทางธุรกิจ ฯลฯ ไปยังภายนอกกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า รวมถึงส่งไปยังอีเมลส่วนตัวโดยไม่ได้รับอนุญาต
- ห้ามมิให้ส่งหรือส่งต่ออีเมลดังต่อไปนี้ ภายในหรือภายนอกกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า :
    - ส่งอีเมลที่มีคำพูดหมิ่นประมาท ทำให้เสียชื่อเสียง ล่วงละเมิด เหยียดเชื้อชาติ หรือ ลามกอนาจาร
    - ส่งอีเมลที่มีไวรัสหรือเวิร์ม
    - ส่งอีเมลจดหมายลูกโซ่ เช่น อีเมลหลอกลวงไวรัสม อีเมลข่าวสารที่ไม่เป็นความจริง, อีเมลการสนับสนุนทางการเมือง หรือ ศาสนา เป็นต้น
    - ส่งอีเมลที่มีเอกสาร ซอฟต์แวร์ หรือข้อมูลอื่น ๆ ที่ละเมิดลิขสิทธิ์ หรือ ความเป็นส่วนตัว

3.2 ผู้ใช้มีหน้าที่ต้องดูแล รักษาทรัพย์สินที่อยู่ในการครอบครอง และส่งคืนทันทีหลังจากสิ้นสุดการใช้งานตามวัตถุประสงค์ หรือ การว่าจ้างสิ้นสุดลง

4. การป้องกันเอกลักษณ์บุคคล

4.1 ห้ามมิให้เปิดเผยข้อมูลสำหรับพิสูจน์ตัวตนที่ออกโดยกลุ่มธุรกิจในเครือซีพี แอ็กซ์ตร้า (รวมถึง hard-token หรือ soft-token)

4.2 ห้ามเขียน ข้อมูลสำหรับการพิสูจน์ตัวตนซึ่งเป็นความลับ เช่น รหัสผ่าน PINS ไว้ในสถานที่ที่ผู้อื่นสามารถมองเห็น

การสร้างรหัสผ่าน

ผู้ใช้ควรเลือกรหัสผ่านที่จำง่าย แต่ยากต่อการคาดเดา โดยใช้แนวทางดังต่อไปนี้

- ไม่ใช้ชื่อ ชื่อย่อ ตัวอักษรย่อของตนเอง ชื่อคนในครอบครัว เพื่อน บริษัท
- ไม่ใช้ข้อมูลส่วนบุคคล เช่น วันเกิด ที่อยู่ หมายเลขโทรศัพท์ ฯลฯ
- ไม่ใช้คำหรือตัวเลข ที่มีรูปแบบที่คาดเดาได้ เช่น aaabbb, qwerty, zyxwvuts, 123321
- ไม่ใช้การเติมตัวเลขนำหน้าหรือตามท้าย (เช่น secret1, 1secret)
- รหัสผ่านที่แข็งแกร่งมีความยาวขั้นต่ำ 8 อักษร ประกอบด้วยตัวเลข (1,2,3) อักขระพิเศษ (@, #, $) และอักษรภาษาอังกฤษตัวพิมพ์เล็ก และใหญ่ (A,B,c)

เพื่อป้องกันความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต

- ผู้ใช้ควรแน่ใจว่า ไม่มีใครเฝ้าดูขณะกำลังป้อนรหัสผ่านเข้าสู่ระบบ
- ผู้ใช้ไม่ถามรหัสผ่านของผู้อื่น
- ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเองภายใต้สถานการณ์ต่อไปนี้
    - เปลี่ยนรหัสผ่านอย่างน้อยหนึ่งครั้งทุก 90 วัน
    - เมื่อระบบบังคับให้เปลี่ยน (โดยระบบงาน และระบบปฏิบัติการ)
    - เปลี่ยนรหัสทันที หลังจากเปิดเผยรหัสผ่านแก่ผู้อื่น หรือสงสัยว่ารหัสผ่านถูกละเมิด

4.3 ห้ามนำเครื่องมือหรืออุปกรณ์ของบุคคลที่สาม มาเชื่อมต่อกับระบบ เว้นแต่ ได้รับการอนุมัติโดยหน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ

5. **การใช้สิทธิระดับสูงโดยมิชอบ** (Privilege misuse)

5.1 ห้ามนำสิทธิ์ระดับสูงไปใช้ในทางมิชอบ

5.2 ผู้ใช้ต้องรายงาน การได้มา หรือการใช้งานสิทธิระดับสูง แก่เจ้าของระบบตามสายบังคับบัญชา และ หรือผู้ดูแลระบบเพื่อรับทราบ

6. **นโยบายการนำอุปกรณ์ไอทีส่วนตัวมาทำงานด้วย** (BYOD)

6.1 ผู้ใช้ทุกคนต้องรับทราบ ข้อกำหนดการใช้งานทรัพย์สินสารสนเทศอย่างถูกต้องปลอดภัย ก่อนนำอุปกรณ์มือถือ อุปกรณ์ไอทีส่วนตัวมาใช้ในที่ทำงาน หรือเข้าถึงอีเมลของบริษัท

6.2 บริษัทมีสิทธิ์ในการควบคุมข้อมูลบริษัท บนอุปกรณ์ไอทีส่วนตัวที่เชื่อมต่อข้อมูลบริษัท เพื่อการป้องกันข้อมูลบริษัทรั่วไหล และการรักษาความปลอดภัยตามนโยบายของบริษัทเท่านั้น

6.3 บริษัทมีสิทธิ์ในการลบข้อมูลของบริษัทเท่านั้น บนอุปกรณ์ไอทีส่วนตัวที่เชื่อมต่อข้อมูลบริษัท เมื่ออยู่ภายใต้สถานการณ์ต่อไปนี้

a) อุปกรณ์ไอทีส่วนตัวสูญหาย หรือ
b) สิ้นสุดสัญญาว่าจ้าง

7. **เครือข่ายทางสังคมออนไลน์ บทความทางอินเทอร์เน็ต กระดานข่าวสาร การแชร์ข้อมูล ฯลฯ**

7.1 ห้ามพนักงานมีปฏิสัมพันธ์ในนามบริษัทผ่านโซเชียลมีเดีย เว้นแต่พนักงานที่ได้รับอนุญาต

7.2 ห้ามโพสต์ข้อมูลของบริษัท หรือ ความคิดเห็นส่วนตัวเกี่ยวกับบริษัทในเครือข่ายสังคม

8. **การปฏิบัติตามระเบียบ**

8.1 พนักงาน และบุคลากรอื่นที่เกี่ยวข้อง ต้องรับทราบข้อกำหนดตามแบบฟอร์มนี้ โดยลงนามในหน้าสุดท้ายของเอกสาร หรือรับทราบผ่านระบบของฝ่ายบุคคล

8.2 การปฏิบัติตามข้อกำหนด และนโยบายที่เกี่ยวข้อง ถือเป็นข้อบังคับ หากละเมิดจะส่งผลให้ถูกลงโทษทางวินัย

8.3 การขาดความเข้าใจในนโยบายเหล่านี้มิถือว่าเป็นเหตุผลของการละเมิดนโยบาย

9. การลงโทษทางวินัย

9.1 การละเมิดข้อกำหนด และ/หรือนโยบายที่กำหนดไว้ จะถูกดำเนินการทางวินัย จากผู้บังคับบัญชา โดยคำแนะนำจากฝ่ายทรัพยากรบุคคล หน่วยงานรักษาความมั่นคงปลอดภัยสารสนเทศ และ/หรือ ฝ่ายที่ดูแลเกี่ยวกับการปฏิบัติตามกฎระเบียบ

9.2 มาตรการทางวินัยอาจมีตั้งแต่การลงโทษให้พนักงานเข้ารับการอบรมซ้ำในเรื่องความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จนไปถึงการยกเลิกการว่าจ้าง