นโยบายเทคโนโลยีสารสนเทศ
และความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท สามารถ เอวิเอชั่น โซลูชั่นส์ จำกัด (มหาชน) และบริษัทย่อย

(ฉบับล่าสุด : ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทฯ เมื่อวันที่ 22 กุมภาพันธ์ 2566)

นโยบายเกี่ยวกับเทคโนโลยีสารสนเทศและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

การใช้งานอุปกรณ์คอมพิวเตอร์ และระบบสารสนเทศของบริษัทฯ

1. ผู้ใช้งานระบบเทคโนโลยีสารสนเทศมีหน้าที่ดูแล รับผิดชอบ และปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยข้อมูลที่กลุ่มบริษัทสามารถ ประกาศใช้อย่างเคร่งครัดและอย่างต่อเนื่องตามขอบเขตที่ตนรับผิดชอบ *(CIP-PL-01 นโยบายเรื่องความมั่นคงปลอดภัยข้อมูลสารสนเทศองค์กร)*
2. ผู้ใช้งานทุกคนมีหน้าที่ดูแลและรับผิดชอบทรัพย์สินต่าง ๆ ของกลุ่มบริษัทสามารถ ที่อยู่ในความครอบครองให้มีความมั่นคงปลอดภัยและอยู่ในสภาพพร้อมใช้งานเสมอ *(CIP-PL-01 นโยบายเรื่องความมั่นคงปลอดภัยข้อมูลสารสนเทศองค์กร)*
3. กลุ่มบริษัทสามารถ สงวนสิทธิ์ในการสุ่มตรวจการใช้งานระบบสารสนเทศของพนักงาน เพื่อความมั่นคงปลอดภัยของข้อมูลโดยรวม
4. ห้ามผู้ใช้งาน ใช้ทรัพย์สิน และระบบเทคโนโลยีสารสนเทศขององค์กร กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม
5. ผู้ใช้งานต้องใช้งานอุปกรณ์คอมพิวเตอร์ของกลุ่มบริษัทสามารถ เพื่อทำงานให้กับองค์กรเท่านั้น ทั้งนี้ จะต้องดูแลรักษาอุปกรณ์เหล่านั้นเป็นอย่างดีเช่นเดียวกับเป็นอุปกรณ์ส่วนตัว และห้ามถอด ปรับปรุง เปลี่ยนแปลง หรือแก้ไขส่วนหนึ่งส่วนใดของอุปกรณ์ด้วยตนเองโดยเด็ดขาด
6. เครื่องคอมพิวเตอร์จะต้องได้รับการปกป้องด้วยรหัสผ่าน หรือ Screen-Saver Password หรือด้วยวิธีการควบคุมอื่น ๆ ทุกครั้งเมื่อไม่ได้ใช้งาน และผู้ใช้งานทุกคนจะต้อง Log-Off จากระบบทุกครั้งเมื่อเสร็จสิ้นการใช้งาน หรือเมื่อจำเป็นต้องหยุดพักการใช้งานชั่วคราว
7. ผู้ใช้งานจะต้องตั้งและใช้งานรหัสผ่านตามวิธีการที่กำหนด *(ACP-WI-02 วิธีปฏิบัติงานเรื่องการสร้างและการใช้งานรหัสผ่าน)* โดยต้องเปลี่ยนรหัสผ่านสำหรับเข้าระบบทันทีที่ทำการเข้าระบบในครั้งแรก ต้องเปลี่ยนรหัสผ่านตามเวลาที่กำหนดและเก็บรักษารหัสผ่านไว้เป็นความลับส่วนบุคคล รวมถึงต้องไม่บันทึกไว้ในโปรแกรมใช้โปรแกรมช่วยจำรหัสผ่าน บอกต่อ แจกจ่าย หรือมอบให้บุคคลอื่นใช้งานในทุก ๆ กรณี
8. ผู้ใช้งานจะต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบในการตรวจสอบการทำงานต่าง ๆ ของเครื่องคอมพิวเตอร์ พร้อมทั้งให้ความร่วมมือในการปฏิบัติตามคำแนะนำจากผู้ดูแลระบบ
9. ห้ามติดตั้งโปรแกรมใด ๆ รวมทั้งโปรแกรมที่ละเมิดลิขสิทธิ์ โปรแกรมประเภท Freeware / Opensource และ Shareware ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ และหากจำเป็นต้องใช้งานโปรแกรม นอกเหนือไปจากที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์ ให้ทำการติดต่อขออนุญาตใช้โปรแกรมและให้ผู้ดูแลระบบเป็นผู้ติดตั้งหรือควบคุมดูแลการติดตั้ง *(SUP-PC-01 ขั้นตอนการปฏิบัติงานเรื่องการติดตั้งโปรแกรมเพิ่มเติม)*
10. โปรแกรมที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ Notebook และอุปกรณ์คอมพิวเตอร์พกพาใด ๆ ที่นำมาใช้ภายในกลุ่มบริษัทสามารถ จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย และเป็นไปตามมาตรฐานที่กลุ่มบริษัทสามารถ กำหนด *(SUP-WI-01 วิธีการปฏิบัติงานเรื่องโปรแกรมมาตรฐานของกลุ่มบริษัทสามารถ)* ทั้งนี้ ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบต่อความผิดใด ๆ อันเกิดจากการละเมิดลิขสิทธิ์โปรแกรมหรือทรัพย์สินทางปัญญาอื่น ๆ ที่เกี่ยวข้อง

11. พนักงานสามารถนำอุปกรณ์ระบบสารสนเทศส่วนบุคคลเข้าในพื้นที่สำนักงานได้ แต่ห้ามทำการเชื่อมต่อเข้ากับระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์อื่น ๆ ในบริเวณพื้นที่สำนักงาน ในกรณีที่ต้องการนำอุปกรณ์ระบบสารสนเทศเข้าพื้นที่สำนักงาน เพื่อเชื่อมต่อกับระบบเครือข่ายหรืออุปกรณ์คอมพิวเตอร์ จะต้องปฏิบัติดังนี้
    - อุปกรณ์ที่จะใช้เพื่อเชื่อมต่อจะต้องได้รับการติดตั้งซอฟต์แวร์ตามที่กำหนดไว้ *(SUP-WI-01วิธีการปฏิบัติงานเรื่องโปรแกรมมาตรฐานของกลุ่มบริษัทสามารถ)*
    - ทั้งนี้ บริษัทฯ ขอสงวนสิทธิ์ในการสุ่มตรวจสอบอุปกรณ์ระบบสารสนเทศที่นำเข้ามาใช้งานตามความเหมาะสม *(CPP-PL-01 นโยบายการปฏิบัติตามนโยบาย กฎระเบียบ และข้อบังคับ)*
12. กรณีที่พนักงานมีการนำอุปกรณ์ระบบสารสนเทศส่วนบุคคล เช่น Notebook Smart Phone หรือ Tablet มาใช้ในการปฏิบัติงานและ/หรือจัดเก็บข้อมูลบริษัทฯ พนักงานจะต้องรักษาความมั่นคงปลอดภัยให้แก่อุปกรณ์นั้นๆ อย่างเหมาะสม เช่นการตั้งรหัสล็อกประจำเครื่องโดยเฉพาะเมื่อมีการนำออกไปใช้งานนอกพื้นที่บริษัทฯ โดยให้ปฏิบัติตาม *(ESP-WI-01 วิธีการปฏิบัติงานเรื่องการใช้งานข้อมูลและอุปกรณ์ภายนอกพื้นที่บริษัท)*
13. ไม่อนุญาตให้นำอุปกรณ์ระบบสารสนเทศเข้าภายในศูนย์ปฏิบัติการสารสนเทศ (Data Center) นอกจากกรณีที่จำเป็นต้องใช้เพื่อการปฏิบัติงาน ซึ่งผู้ใช้งานจะต้องขออนุญาตใช้งานและปฏิบัติตาม *(ESP-PC-01 ขั้นตอนการปฏิบัติงานเรื่องการควบคุมการนำอุปกรณ์สารสนเทศเข้าใช้งานในพื้นที่)*
14. บริษัทฯ อนุญาตให้มีการนำอุปกรณ์ระบบสารสนเทศต่าง ๆ ออกไปใช้งานนอกพื้นที่ได้ในกรณีที่มีความจำเป็น โดยพนักงานผู้ที่ต้องการนำอุปกรณ์ระบบสารสนเทศออกไปใช้งานจะต้องขออนุมัติและปฏิบัติตาม *(ESP-PC-02 ขั้นตอนการปฏิบัติงานเรื่องการนำอุปกรณ์สารสนเทศออกนอกบริเวณหน่วยงานศูนย์บริการสารสนเทศ)* โดยการนำอุปกรณ์ระบบสารสนเทศออกไปใช้งานนอกพื้นที่นี้ พนักงานจะต้องระมัดระวังและดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินของบริษัทฯ อย่างเหมาะสม *ตาม (ESP-WI-01 วิธีการปฏิบัติงานเรื่องการใช้งานข้อมูลและอุปกรณ์ภายนอกพื้นที่บริษัท)*
15. ผู้ใช้งานจะต้องใช้งานระบบอีเมล์ ของกลุ่มบริษัทสามารถ เพื่อติดต่อประสานงานทางด้านธุรกิจของกลุ่มบริษัทสามารถ เท่านั้น และขนาดของข้อมูลที่ใช้ในการรับ ส่ง และจัดเก็บ จะต้องเป็นไปตามมาตรฐานที่กลุ่มบริษัทสามารถ กำหนดไว้
16. ห้ามใช้ที่อยู่ Email Address ของบริษัทฯ ในการสมัครจดหมายข่าวหรือให้ข้อมูลกับ Website หรือ Web board ที่ไม่เกี่ยวข้องกับการทำงาน
17. ผู้ใช้งานจะต้องใช้โปรแกรมอีเมล์ ที่กลุ่มบริษัทสามารถ จัดหาและอนุญาตให้ใช้ในการเชื่อมต่อกับระบบอีเมล์ของกลุ่มบริษัทสามารถ เท่านั้น
18. ห้ามใช้งานระบบอีเมล์ ในการส่ง หรือส่งต่อ (forward) ไปยังผู้รับจำนวนมาก หรือในลักษณะลูกโซ่ ยกเว้นในกรณีที่ได้รับอนุญาตให้สามารถกระทำได้
19. ห้ามผู้ใช้งานทำการเก็บรักษา ส่ง หรือส่งต่ออีเมล์ ที่มีเนื้อหาหรือไฟล์แนบที่ไม่เหมาะสม เช่น ไฟล์แนบที่เป็นรูปภาพลามกอนาจาร หรือไฟล์แนบที่ละเมิดลิขสิทธิ์ของผู้อื่น เป็นต้น
20. ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ E-mail ของบุคคลอื่นโดยเด็ดขาด

21. ห้ามพนักงานนำข้อมูลที่เกี่ยวข้องกับบริษัทฯ และธุรกิจ เผยแพร่ออกไปภายนอก ไม่ว่าจะทางตรงและทางอ้อม เช่น ทางอินเทอร์เน็ต หรือ Social Network เป็นต้น

22. การเข้าใช้งานอินเตอร์เน็ต ต้องเข้าใช้งานผ่านช่องทางที่บริษัทฯ จัดหาไว้ให้เท่านั้น โดยบริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเตอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานที่ไม่เหมาะสม

23. อนุญาตให้ใช้งานระบบอินเทอร์เน็ตของกลุ่มบริษัทสามารถ เพื่อการทำงานและเพื่อเพิ่มประสิทธิภาพในการทำงานเท่านั้น ห้ามใช้เพื่อประโยชน์ส่วนตัว และเข้าเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่มีภาพลามกอนาจาร การพนัน ฟังเพลง ดูภาพยนตร์/คลิป เล่นเกม ดาวน์โหลด อัพโหลด หางาน เว็บไซต์ที่มีเนื้อหาหมิ่นสถาบันพระมหากษัตริย์ เว็บไซต์ที่ผิดกฎหมาย หรือเว็บไซต์ที่มีเนื้อหาขัดต่อความมั่นคงของชาติ เป็นต้น

24. ห้ามติดตั้งหรือใช้งานอุปกรณ์ประเภทอุปกรณ์สื่อสารข้อมูลอื่นใด (เช่น ระบบ 3G, 4G, Wi-Fi เป็นต้น) เพื่อเชื่อมต่อออกสู่ระบบเครือข่ายภายนอก โดยไม่ได้รับอนุญาต หากจำเป็นต้องใช้งานอุปกรณ์ดังกล่าวจะต้องได้รับการอนุญาตตามขั้นตอนที่กำหนดไว้ *(NMP-PL-01 นโยบายเรื่องการจัดการเครือข่าย)*

25. พนักงานที่ต้องการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ติดตั้งอยู่ในศูนย์บริการสารสนเทศของกลุ่มบริษัทสามารถ เพื่อปฏิบัติงานจากสถานที่อื่น ๆ ภายนอกองค์กร จะต้องได้รับอนุญาตจากหัวหน้างานของตน และผู้บริหารของศูนย์บริการสารสนเทศ *(NMP-PL-01 นโยบายเรื่องการจัดการเครือข่าย)*

26. การใช้งานเครือข่ายไร้สาย หรือเปิดใช้งานฟังก์ชั่นการสื่อสารไร้สาย (เช่น Wireless LAN, Bluetooth) บนอุปกรณ์ระบบสารสนเทศทุกประเภท ในบริเวณพื้นที่สำนักงานจะต้องทำการลงทะเบียนอุปกรณ์และได้รับอนุญาตจากผู้ดูแลระบบ และจะต้องใช้งานภายในบริเวณพื้นที่ที่กำหนดไว้เท่านั้น *(NMP-PL-01 นโยบายเรื่องการจัดการเครือข่าย)*

27. ผู้ใช้งานจะต้องไม่เจตนาสร้าง เปิดทำงาน หรือส่งต่อ โปรแกรมที่เป็นภัยคุกคาม เช่น โปรแกรมไวรัสหรือเวิร์ม เป็นต้น และห้ามปิดหรือยกเลิกการทำงานของโปรแกรมตรวจจับภัยคุกคามของเครื่องคอมพิวเตอร์ที่ใช้งาน

28. ในกรณีที่พนักงานได้รับคำสั่งให้โอนย้ายไปปฏิบัติงานยังบริษัทอื่นที่อยู่ในเครือ พนักงานจะต้องแจ้งให้หน่วยงาน IT รับทราบ เพื่อทำการโอนย้ายทรัพย์สินในระบบ และพนักงานต้องไม่ทำการเคลื่อนย้าย หรือนำเครื่องคอมพิวเตอร์ติดตัวไปด้วย

29. พนักงานจะต้องไม่ทำการปรับปรุง/แก้ไข/ถอดถอน อุปกรณ์คอมพิวเตอร์ของบริษัทฯ หากต้องการ ปรับปรุง/แก้ไข/ถอดถอน อุปกรณ์คอมพิวเตอร์จะต้องแจ้งกับหน่วยงาน IT ให้เป็นผู้ดำเนินการเท่านั้น

30. พนักงานจะต้องไม่ติดตั้งโปรแกรมลิขสิทธิ์และโปรแกรมอื่นๆเพิ่มเติม หากฝ่าฝืนต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และความรับผิดชอบทางกฎหมายที่เกิดขึ้นจากการกระทำการฝ่าฝืนดังกล่าวด้วย

31. ก่อนที่พนักงานจะพ้นสภาพจากการเป็นพนักงานของบริษัทที่สังกัด หรือบริษัทในเครือ พนักงานจะต้องส่งคืน Notebook ให้กับส่วนงาน HR ก่อนวันทำงานวันสุดท้ายไม่น้อยกว่า 2 วันทำการและในกรณีคอมพิวเตอร์ PC พนักงานจะต้องแจ้งหน่วยงาน IT ทราบก่อนวันทำงานวันสุดท้ายไม่น้อยกว่า 2 วันทำการ หากอุปกรณ์คอมพิวเตอร์เกิดการสูญหาย เสียหาย พนักงานจะต้องรับผิดชอบและชดใช้ราคาอุปกรณ์คอมพิวเตอร์ตามราคาที่หน่วยงาน IT ประเมิน หากพนักงานเพิกเฉยไม่รับผิดชอบชดใช้ราคาดังกล่าว พนักงานอาจจะถูกดำเนินคดีได้

เอกสารที่เกี่ยวข้อง

1. CIP-PL-01 : นโยบายเรื่องความมั่นคงปลอดภัยข้อมูลสารสนเทศองค์กร
2. ACP-WI-02 : วิธีปฏิบัติงานเรื่องการสร้างและการใช้งานรหัสผ่าน
3. SUP-PC-01 : ขั้นตอนการปฏิบัติงานเรื่องการติดตั้งโปรแกรมเพิ่มเติม
4. SUP-WI-01 : วิธีการปฏิบัติงานเรื่องโปรแกรมมาตรฐานของกลุ่มบริษัทสามารถ
5. CPP-PL-01 : นโยบายการปฏิบัติตามนโยบาย กฎระเบียบ และข้อบังคับ
6. ESP-PC-01 : ขั้นตอนการปฏิบัติงานเรื่องการควบคุมการนำอุปกรณ์สารสนเทศเข้าใช้งานในพื้นที่
7. ESP-PC-02 : ขั้นตอนการปฏิบัติงานเรื่องการนำอุปกรณ์สารสนเทศออกนอกบริเวณหน่วยงาน ศูนย์บริการสารสนเทศ
8. NMP-PL-01 : นโยบายเรื่องการจัดการเครือข่าย