



นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
(Information Security Policy)

บริษัท ชันสวีท จำกัด

สารบัญ

	หน้า
1. นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)	3
2. นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)	3
3. นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)	4
4. นโยบายความมั่นคงปลอดภัยของอีเมล (E-mail Policy)	5
5. นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)	6
6. นโยบายความมั่นคงปลอดภัยการใช้งานระบบคอมพิวเตอร์ (Computer Security Policy)	7

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (Acceptable Use Policy)

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศบริษัทชั้นสวีท จำกัด เป็นการจัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทชั้นสวีท จำกัด ให้อยู่ระดับมาตรฐานสากลโดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของบริษัทชั้นสวีท จำกัด

นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

1. ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตพื้นที่ที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
2. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (WiFi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย
3. ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน
4. ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1. ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ภายในส่วนกลาง
2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด
3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท ที่ไม่อนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์
4. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
5. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
6. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทางบริษัทให้ใช้งาน ซึ่งหาก มีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อ นอกเหนือที่กำหนด จะต้องได้รับความความยินยอมจาก แผนกเทคโนโลยีสารสนเทศก่อน
7. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดย ข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง
8. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์ทุกครั้งที่มีการเปลี่ยนแปลงค่า
9. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป
10. แผนกเทคโนโลยีสารสนเทศ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข
11. ข้อกำหนดการลงโทษผู้ซึ่งมิได้ปฏิบัติตามนโยบายด้านความปลอดภัยของไฟร์วอลล์
 - 11.1. ให้ดำเนินการกล่าวตักเตือนด้วยวาจากับผู้ใช้งาน
 - 11.2. ในกรณีที่ผู้ใช้งานยังคงไม่ปฏิบัติตามนโยบายและยังคงปฏิบัติอยู่เช่นเดิม ให้ดำเนินการตักเตือนเป็นลายลักษณ์อักษรถึงผู้บังคับบัญชา

นโยบายความมั่นคงปลอดภัยของอีเมล (E-mail Policy)

1. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) ของหน่วยงาน โดยยื่นคำขอกับเจ้าหน้าที่ดูแลระบบ (E-mail)
2. จะมีการเปลี่ยนแปลง Password ทุก ๆ 6 เดือน
3. ห้ามมิให้เจ้าหน้าที่ผู้ไม่มีสิทธิเข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
4. ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ ไว้ตามที่อยู่เว็บไซต์ต่าง ๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร
5. ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
6. ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
7. ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
8. ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
9. ห้ามปลอมหรือปิดชื่อที่อยู่ E-mail ของตน เมื่อทำการส่งจดหมายไปยังผู้รับหนึ่ง
10. ห้ามส่ง E-mail ที่มีลักษณะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น
11. ห้ามปลอมแปลง E-mail ของบุคคลอื่น
12. ห้ามรับ หรือส่ง E-mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
13. ให้ใช้คำที่สุภาพในการส่ง E-mail
14. ห้ามส่ง E-mail ที่มีขนาดใหญ่เกินกว่า 5 เมกกะไบต์ หรือตามที่องค์กรระบุไว้
15. ห้ามส่ง E-mail ที่เป็นความลับขององค์กร เว้นเสียแต่จะใช้วิธีการเข้ารหัสข้อมูล E-mail ที่องค์กรกำหนดไว้
16. ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-mail ของผู้รับให้ถูกต้อง
17. ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้รับทราบ
ให้ทำการสำรองข้อมูล E-mail ตามความจำเป็นอย่างสม่ำเสมอ
18. ห้ามใช้ E-mail ส่วนตัวมาใช้ในการทำงานโดยเด็ดขาด

นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

1. ห้ามใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระเทยกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อ สังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน
2. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านระบบอินเทอร์เน็ต (Internet)
3. ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ หน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ
4. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งาน โดยบุคคลอื่น ๆ
5. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ บริษัทชั้นสวีท จำกัด การ พยายามเข้าถึงระบบ โดยมีขอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบ สารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่ สอดคล้องกับ พรบว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พศ.2550 หรือเป็นการกระทำที่ ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของ บริษัทชั้นสวีท จำกัด จะต้องถูกดำเนินคดี ตามขั้นตอนของกฎหมาย

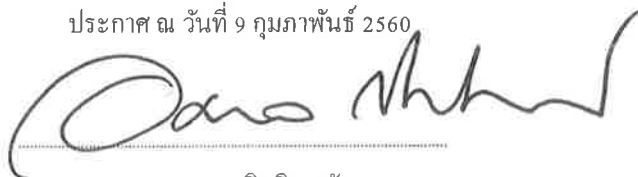
นโยบายความมั่นคงปลอดภัยการใช้งานระบบคอมพิวเตอร์ (Computer Security Policy)

1. User Account และ Password เป็นความลับเฉพาะส่วนบุคคล ห้ามให้บุคคลอื่นใช้ และผู้ขอใช้บริการต้องรับผิดชอบการกระทำใด ๆ ที่เกิดจากการใช้งานบัญชีดังกล่าว
2. เมื่อได้ User Account และ Password ครั้งแรก ระบบจะบังคับให้เปลี่ยน Password ใหม่ทันที
3. ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 6 ตัวอักษร
4. จะต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 1 เดือน
5. การเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
6. ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 5 ครั้ง
7. ห้ามผู้ใช้งานทำการเคลื่อนย้าย ติดตั้ง ซ่อมแซม เปลี่ยนแปลงการตั้งค่า หรือดัดแปลง ชิ้นส่วนอุปกรณ์ของระบบคอมพิวเตอร์ ภายในองค์กรโดยเด็ดขาด
8. ห้ามมิให้พนักงานติดตั้ง โปรแกรมทุกชนิด หรืออุปกรณ์ต่อพ่วงอื่นใด นอกเหนือจากที่บริษัทได้จัดไว้ให้ กรณีมีความจำเป็นต้องติดตั้ง ให้แจ้งผู้ดูแลระบบเป็นผู้ดำเนินการให้
9. การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์ส่วนตัวอื่นใดเข้ามาเชื่อมต่อกับอุปกรณ์คอมพิวเตอร์และเครือข่ายของบริษัท จะต้องได้รับอนุญาตจากผู้ดูแลระบบ หรือหน่วยงานผู้รับผิดชอบอุปกรณ์คอมพิวเตอร์และเครือข่าวนั้น ๆ ก่อนเท่านั้น
10. ห้ามใช้ระบบคอมพิวเตอร์ เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการทำงาน
11. ห้าม Download/ Upload ข้อมูลหรือสิ่งใดที่ไม่เกี่ยวข้องกับงาน หรือใช้ Website ที่ไม่เกี่ยวข้องกับงาน
12. ห้ามจัดเก็บไฟล์,รูปภาพ,เพลง,วิดีโอ,เกม หรือ โปรแกรมที่ไม่เกี่ยวข้องกับงาน ซึ่งทำให้เปลืองพื้นที่จัดเก็บ ลงในระบบคอมพิวเตอร์
13. ห้ามโอนย้าย สำเนา นำออก ซึ่งไฟล์ หรือข้อมูลใดๆขององค์กร ให้ภายนอกโดยไม่ได้รับอนุญาตจากผู้จัดการฝ่าย

14. กรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกบริษัทจะต้องได้รับอนุมัติจากผู้มีอำนาจในการนำทรัพย์สินออกก่อนทุกครั้ง
15. ห้ามใช้ระบบคอมพิวเตอร์ ในการพยายามเข้าถึง ไฟล์ ข้อมูล ฐานข้อมูล อีเมลล์ของบุคคล สถาบัน หรือ บริษัท โดยไม่มีสิทธิ์ หรือไม่ได้รับอนุญาตจากเจ้าของ
16. ให้ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติ และ มีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติให้รีบแจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไขโดยทันที
17. ปิดเครื่องคอมพิวเตอร์ทันทีหลังเลิกงาน หรือเมื่อไม่ได้ใช้งานนานเกินกว่า 2 ชั่วโมง
18. ผู้ใช้งานคอมพิวเตอร์ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

ทั้งนี้ มีผลตั้งแต่วันนี้เป็นต้นไป

ประกาศ ณ วันที่ 9 กุมภาพันธ์ 2560



(นายองอาจ กิตติคุณชัย)

ประธานเจ้าหน้าที่บริหาร