บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ มีระบบเทคโนโลยีสารสนเทศเพื่อใช้ในการอำนวยความสะดวกและเพิ่มศักยภาพในการปฏิบัติงาน จึงกำหนดแนวทางในการใช้งานระบบเทคโนโลยีสารสนเทศให้มีความเหมาะสม มีการบริหารทรัพยากรระบบเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ และมีการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง รวมถึงการป้องกันการถูกคุกคามจากภัยต่างๆที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังนี้

ขอบเขตนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์ของนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ มีดังนี้

1. เพื่อให้เกิดความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ
2. เพื่อกำหนดวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ ผู้ใช้บริการระบบเทคโนโลยีสารสนเทศ และผู้ที่เกี่ยวข้อง
3. เพื่อสร้างความตระหนักในความสำคัญในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
4. เพื่อให้มีการตรวจสอบและมีการประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ ประกอบด้วย

ข้อ 1 คำนิยาม
ข้อ 2 อำนาจและหน้าที่
ข้อ 3 การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ข้อ 4 สิทธิและความปลอดภัยในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
ข้อ 5 นโยบายการป้องกันข้อมูลสารสนเทศ
ข้อ 6 ขั้นตอนในการปฏิบัติเพื่อความปลอดภัยในระบบเทคโนโลยีสารสนเทศ
ข้อ 7 ระเบียบการใช้ Internet และ Email
ข้อ 8 นโยบายการบริหารและการป้องกันระบบเทคโนโลยีสารสนเทศ
ข้อ 9 นโยบายการป้องกันและกู้คืนระบบเทคโนโลยีสารสนเทศ
ข้อ 10 ข้อปฏิบัติของผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ
ข้อ 11 บทลงโทษและการบังคับใช้

คำนิยาม

คำนิยามในนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ มีดังนี้

"บริษัท" หมายถึง บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน) และบริษัทในเครือ

"ระบบเทคโนโลยีสารสนเทศ" หมายถึง Hardware คอมพิวเตอร์ เช่น Server, Workstation Computer, Desktop Computer, Laptop Computer, Smart Device, Tablet, Printer, Scanner เป็นต้น หรือเป็น Software คอมพิวเตอร์ เช่น Virtual Machine, ฐานข้อมูล, โปรแกรมสำเร็จรูป, โปรแกรมที่ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้พัฒนา เป็นต้น และยังรวมถึงระบบเครือข่ายเทคโนโลยีสารสนเทศ

"ระบบเครือข่ายเทคโนโลยีสารสนเทศ" หมายถึง การติดต่อสื่อสารหรือการส่งข้อมูลระหว่างกัน ทั้งภายในบริษัท และภายนอกบริษัท เช่น Internet, Router, Firewall, Network Switching, Wired Network, Wireless Network, Wireless Access Point เป็นต้น

"ประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่" หมายถึง ประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่ บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน)

"พนักงาน" หมายถึง พนักงานและลูกจ้างของบริษัท รวมถึงบุคคลอื่นที่บริษัทมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง หรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบใดๆก็ตาม หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ เช่น เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย รูปภาพ ภาพเคลื่อนไหว การบันทึกภาพหรือเสียง การบันทึกโดยใช้เครื่องคอมพิวเตอร์ เป็นต้น

"ผู้ดูแลระบบเทคโนโลยีสารสนเทศ" หมายถึง ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ โดยได้รับมอบหมายจากประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่ ให้มีหน้าที่รับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และสามารถเข้าถึงโปรแกรมระบบเทคโนโลยีสารสนเทศ เพื่อการจัดการฐานข้อมูลของเครือข่ายระบบเทคโนโลยีสารสนเทศ ทั้งนี้ อาจมอบหมายให้พนักงานฝ่ายเทคโนโลยีสารสนเทศดำเนินการแทนตามความเหมาะสม

" ความลับ " หมายถึง สื่อสารสนเทศที่จัดเก็บในรูปแบบของข้อมูล หรือข่าวสารที่บันทึกไว้ในรูปแบบใดๆก็ตาม โดยมีการจัดลำดับและความสำคัญของเนื้อหาและจำกัดการเข้าถึง หรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงสื่อบันทึกต่างๆ รหัสผ่าน บัญชีเข้าใช้ หรือเอกสารทุกเรื่องที่บันทึกเรื่องดังกล่าว

อำนาจและหน้าที่

ข้อ 1 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ดังต่อไปนี้

1.1 กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลระบบเทคโนโลยีสารสนเทศ
1.2 ให้คำปรึกษาและคำแนะนำแก่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ
1.3 ให้คำเสนอแนะต่อประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่ในการกำหนดนโยบายและมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
1.4 นำเสนอผลการปฏิบัติงานต่อประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่
1.5 ปฏิบัติหน้าที่อื่นตามที่ประธานเจ้าหน้าที่บริหารกลุ่ม/กรรมการผู้จัดการใหญ่มอบหมาย
1.6 รักษาความมั่นคงปลอดภัยและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ข้อ 2 เจ้าหน้าที่ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ มีหน้าที่ดังต่อไปนี้

2.1 ดูแลการใช้ระบบเครือข่ายเทคโนโลยีสารสนเทศ
2.2 ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวข้องกับระบบเครือข่ายเทคโนโลยีสารสนเทศ
2.3 กำหนดบัญชีผู้เข้าใช้งานระบบเครือข่ายเทคโนโลยีสารสนเทศ
2.4 รักษาความมั่นคงปลอดภัยและประเมินความเสี่ยงของระบบเครือข่ายเทคโนโลยีสารสนเทศ

ข้อ 3 เจ้าหน้าที่พัฒนาโปรแกรม มีหน้าที่ดังต่อไปนี้

3.1 พัฒนาโปรแกรมตามที่ได้รับมอบหมาย
3.2 จัดเตรียมข้อมูลทดสอบเพื่อใช้ในการทดสอบความถูกต้องของโปรแกรม
3.3 ดูแล บำรุงรักษา ปรับปรุงโปรแกรมที่พัฒนา ให้ทันสมัยและพร้อมใช้งานอยู่ตลอดเวลา
3.4 มีความมั่นคงปลอดภัยของโปรแกรม มีการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ข้อ 4 เจ้าหน้าที่บริการเทคโนโลยีสารสนเทศ มีหน้าที่ดังต่อไปนี้

4.1 ควบคุม ดูแลการใช้งานอุปกรณ์ คอมพิวเตอร์สำนักงานของบริษัท
4.2 ควบคุมและตรวจสอบการติดตั้งโปรแกรมที่เข้าสู่ระบบเทคโนโลยีสารสนเทศให้เป็นไปตามวัตถุประสงค์ของบริษัท
4.3 รับผิดชอบงานบริการเทคโนโลยีสารสนเทศ เช่น การซ่อมบำรุงรักษา การแก้ไขปัญหา การปรับปรุง การตรวจสอบไวรัสคอมพิวเตอร์ การให้คำแนะนำวิธีการใช้งาน เป็นต้น

4.4 ให้คำแนะนำและส่งเสริมให้พนักงานของบริษัท มีความรู้และปฏิบัติตามกระบวนการเข้าใช้งานระบบเทคโนโลยีสารสนเทศที่ถูกต้อง

4.5 จัดทำรายการอุปกรณ์ สถานะการใช้งาน ตลอดจนการใช้งานของอุปกรณ์คอมพิวเตอร์

4.6 ลดความเสี่ยงจากการรั่วไหลของข้อมูล เมื่ออุปกรณ์คอมพิวเตอร์ชำรุดหรือหมดอายุการใช้งาน โดยการทำลายข้อมูลอย่างถูกต้องและต้องไม่สามารถกู้คืนข้อมูลกลับมาได้ และกำหนดวิธีการทำลายทรัพย์สินเพื่อให้เกิดมูลค่าสูงสุด โดยต้องคำนึงถึงผลกระทบกับสิ่งแวดล้อม เช่น การรีไซเคิ้ล เป็นต้น

การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

- **ห้อง** Data Center

ห้อง Data Center ใช้เป็นที่ตั้งของระบบเทคโนโลยีสารสนเทศของบริษัท ซึ่งประกอบด้วย

1. ระบบ Server
2. ระบบการรักษาความปลอดภัยของระบบเครือข่ายเทคโนโลยีสารสนเทศ
3. ระบบการเชื่อมต่อระบบเครือข่ายเทคโนโลยีสารสนเทศ
4. ระบบการสำรองกระแสไฟฟ้า ให้กับอุปกรณ์ทั้งหมดในห้อง Data Center
5. ระบบการควบคุมอุณหภูมิภายในห้อง ให้เหมาะสมสำหรับอุปกรณ์ทั้งหมดในห้อง Data Center
6. ระบบควบคุมการเข้าห้อง Data Center
7. ระบบควบคุมอุปกรณ์ดับเพลิงภายในห้อง ให้เหมาะสมกับอุปกรณ์ทั้งหมดในห้อง Data Center
8. ระบบการบริหารจัดการอุปกรณ์คอมพิวเตอร์ทั้งหมดของบริษัท
9. ระบบการสำรองข้อมูลแบบภายในและระบบการสำรองข้อมูลไปยังศูนย์คอมพิวเตอร์สำรอง
10. ระบบกล้องวงจรปิด ภายในห้อง Data Center

ดังนั้น ห้อง Data Center จึงถือเป็นห้องปฏิบัติการที่มีความสำคัญของบริษัท จึงมีความจำเป็นต้องรักษาความมั่นคงปลอดภัยของห้อง Data Center อย่างเข้มงวด จึงกำหนดระเบียบปฏิบัติ ดังนี้

ข้อ 1 ห้อง Data Center มีทางเข้าอยู่ทิศทางเดียวซึ่งอยู่ในสภาพที่ปิดห้อง Data Center ตลอดเวลา และมีระบบรักษาความปลอดภัยที่เหมาะสม

ข้อ 2 ผู้เข้าห้อง Data Center ต้องเป็นผู้มีสิทธิ์เข้าปฏิบัติงานเท่านั้น ผู้มีสิทธิ์เข้าห้อง Data Center ประกอบด้วย ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ผู้ที่ได้รับมอบหมายให้ดำเนินการ หรือบุคคลภายนอกที่มีหน้าที่ติดตั้งระบบ ซ่อมแซมระบบ หรือบำรุงรักษาระบบ โดยผู้ที่ได้รับมอบหมายต้องควบคุมและติดตามการทำงานของบุคคลภายนอกตลอดเวลาที่ทำงานในห้อง Data Center

ข้อ 3 การเข้าห้อง Data Center ต้องยืนยันตัวตนผ่านอุปกรณ์ควบคุมการเข้าห้อง Data Center โดยอุปกรณ์ควบคุมดังกล่าวต้องสามารถบันทึกประวัติการเข้าห้อง Data Center ได้

ข้อ 4 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ตรวจสอบประวัติการเข้าห้อง Data Center เป็นประจำทุกเดือน

ข้อ 5 ห้อง Data Center ต้องมีระบบควบคุมอุณหภูมิภายในห้อง Data Center ให้เหมาะสมกับอุปกรณ์ทั้งหมดในห้อง Data Center และมีการบำรุงรักษาระบบควบคุมอุณหภูมิเป็นประจำทุกปี

ข้อ 6 ห้อง Data Center ต้องมีระบบสำรองการควบคุมอุณหภูมิ เพื่อใช้ทดแทนในกรณีที่ระบบหลักไม่สามารถใช้งานได้ และสามารถตรวจสอบอุณหภูมิของห้อง Data Center จากระยะไกลได้ตลอดเวลา

ข้อ 7 ห้อง Data Cener ต้องมีระบบสำรองกระแสไฟฟ้าและระบบป้องกันกระแสไฟกระชากให้เหมาะสมกับอุปกรณ์ทั้งหมดในห้อง Data Center และมีการทดสอบระบบสำรองกระแสไฟฟ้าเป็นประจำทุกปี

ข้อ 8 ห้อง Data Center ต้องมีระบบดับเพลิงที่เหมาะสมและมีการทดสอบระบบดับเพลิงเป็นประจำทุกปี

ข้อ 9 ห้อง Data Center ต้องมีระบบกล้องวงจรปิดที่สามารถบันทึกการปฏิบัติงานของผู้ที่เข้าห้อง Data Center มีการเก็บรักษาข้อมูลกล้องวงจรปิด และสามารถดูภาพของกล้องวงจรปิดจากระยะไกลได้ตลอดเวลา

ข้อ 10 ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าในห้อง Data Center โดยเด็ดขาด

- **เครื่องคอมพิวเตอร์ส่วนบุคคล**

พนักงานบริษัท ที่มีการใช้เครื่องคอมพิวเตอร์ของบริษัท มีระเบียบปฏิบัติดังนี้

ข้อ 1 การเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท ให้ใช้บัญชีผู้เข้าใช้งานของตนเองเท่านั้น

ข้อ 2 พนักงานพึงดูแลและรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงอันเป็นทรัพย์สินของบริษัท ให้อยู่ในสภาพที่ดีและพร้อมใช้งาน ไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์ และใช้งานอย่างมีประสิทธิภาพ

ข้อ 3 ข้อมูลที่มีความสำคัญต้องจัดเก็บไว้ในที่ปลอดภัยหรือป้องกันการเข้าถึงได้โดยง่าย

ข้อ 4 การติดตั้งโปรแกรมเพิ่มเติมตามความจำเป็นของผู้ใช้ ต้องได้รับการอนุมัติจากต้นสังกัดก่อน การติดตั้งโปรแกรมให้ดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

ข้อ 5 ห้ามพนักงานติดตั้งโปรแกรมหรือใช้โปรแกรมที่เป็นการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาของผู้อื่นบนเครื่องคอมพิวเตอร์ของบริษัท และห้ามใช้โปรแกรมที่เป็นการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาของผู้อื่นบนเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเองบนระบบเครือข่ายของบริษัทหรือมีการใช้ Email ของบริษัทในเครื่องคอมพิวเตอร์ หากมีการร้องเรียนค่าเสียหายจากการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา ผู้ที่ละเมิดต้องเป็นผู้รับผิดชอบเป็นการส่วนตัวที่ได้กระทำการอันเป็นความผิดตามกฎหมาย

ข้อ 6 ห้ามพนักงานดัดแปลง แก้ไข ถอดอุปกรณ์ ปรับปรุงอุปกรณ์ หรือเพิ่มเติมอุปกรณ์ในระบบเทคโนโลยีสารสนเทศ หรือโปรแกรมที่บริษัทจัดให้ นอกเหนือจากอุปกรณ์ปกติที่บริษัทจัดให้โดยไม่ได้รับอนุญาต หากมีความจำเป็น ต้องดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

ข้อ 7 ห้ามบุคคลภายนอกใช้งานอุปกรณ์คอมพิวเตอร์ของบริษัท หากมีความจำเป็นให้ทำการร้องขอฝ่ายเทคโนโลยีสารสนเทศเพื่อให้บริการดังกล่าว

<u>สิทธิและความปลอดภัยในการเข้าใช้ระบบเทคโนโลยีสารสนเทศ</u>

ข้อควรปฏิบัติของพนักงานผู้ที่ได้สิทธิในการเข้าใช้ระบบเทคโนโลยีสารสนเทศของบริษัท มีดังนี้

- **รหัสบัญชีผู้ใช้งาน สำหรับพนักงาน**

การสร้างบัญชีผู้ใช้งานจะถูกกำหนดตามคำร้องขอและต้องได้รับการอนุมัติจากต้นสังกัดก่อน โดยประเภทของการเข้าถึงข้อมูล สิทธิ์ในการเข้าถึงข้อมูล ลำดับชั้นความลับของข้อมูล ต้องเป็นไปตามความจำเป็นในการใช้ทรัพยากรสารสนเทศของบริษัท ซึ่งอยู่ในดุลยพินิจของผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ที่สามารถเปลี่ยนแปลงสิทธิ์ของผู้ใช้งานให้แตกต่างจากคำร้องขอได้ เพื่อให้ตรงกับความจำเป็นในทางการดำเนินกิจกรรมซึ่งเอื้อประโยชน์ต่อการดำเนินธุรกิจของบริษัท หมายความรวมถึง การตั้งค่าในระบบเครือข่ายสารสนเทศ การใช้ฐานข้อมูล การใช้ทรัพยากรของบริษัทร่วมกัน การใช้งานจากเครือข่ายจากพื้นที่นอกสำนักงาน รวมถึงการกำหนดวิธีการใช้ Email ของบริษัท

- **ระบบบัญชีผู้ใช้งาน สำหรับผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ**

การตั้งค่าต่างๆของบัญชีผู้ใช้งาน ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ การร้องขอการใช้งานต่างๆบนระบบเครือข่ายเพิ่มเติมจะกระทำได้หากการดำเนินกิจกรรมนั้นเพื่อเอื้อประโยชน์ต่อการดำเนินธุรกิจของบริษัท ซึ่งในการเปลี่ยนแปลงค่าต่างๆในระบบ ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบเท่านั้น

- **ข้อพึงปฏิบัติ**

ข้อ 1 พนักงานพึงใช้ทรัพยากรเครือข่ายเทคโนโลยีสารสนเทศอย่างเหมาะสมและมีประสิทธิภาพ

ข้อ 2 พนักงานต้องใช้ข้อความสุภาพในการติดต่อสื่อสารระหว่างกัน และถูกต้องตามธรรมเนียมปฏิบัติสากล การส่ง Email แบบกระจายถึงทุกคนให้ใช้ได้เฉพาะที่เกี่ยวข้องกับการปฏิบัติงานเท่านั้น

ข้อ 3 พนักงานมีหน้าที่ระมัดระวังและรักษาความปลอดภัยในการใช้เครือข่ายเทคโนโลยีสารสนเทศ โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

- **รหัสผ่านส่วนบุคคล**

การใช้รหัสผ่านส่วนบุคคล พนักงาน ต้องปฏิบัติดังต่อไปนี้

ข้อ 1 การกำหนดรหัสผ่านส่วนบุคคล ต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยรหัสผ่านต้องมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลที่มาจากชื่อหรือนามสกุลของตนเอง หรือบุคคลภายในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม หรือหมายเลขโทรศัพท์ ทะเบียนรถ เลขที่บัตรประชาชน เลขที่บ้านของตนเอง หรือเป็นรหัสผ่านที่สามารถคาดเดาได้อย่างง่าย เช่น P@ssw0rd, Abc!23, !L0veyou, Le!me1n เป็นต้น

ข้อ 2 กรณีใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายเทคโนโลยีสารสนเทศ ต้องบันทึกรหัสผ่านด้วยตนเองเท่านั้น ไม่อนุญาตให้ใช้โปรแกรมคอมพิวเตอร์ Save Password ไว้เพื่อช่วยในการจำรหัสผ่านของตนเองแบบอัตโนมัติ

ข้อ 3 ห้ามพนักงานเปิดเผยรหัสส่วนบุคคลของตนเองให้ผู้อื่นทราบ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นจากบุคคลอื่นได้

ข้อ 4 ต้องเปลี่ยนรหัสผ่านส่วนบุคคลในการเข้าใช้งานระบบเครือข่ายเทคโนโลยีสารสนเทศทุกๆ 90 วัน

ข้อ 5 ต้องเปลี่ยนรหัสผ่านส่วนบุคคลในการเข้าใช้งานระบบ ERP และระบบบริหารงานบุคคลทุกๆ 60 วัน

ข้อ 6 กรณีที่พนักงานลืมรหัสผ่าน ให้ร้องขอรหัสผ่านใหม่โดยใช้เครื่องมือเปลี่ยนรหัสผ่านด้วยตนเอง หรือแจ้งฝ่ายเทคโนโลยีสารสนเทศให้ดำเนินการ

ข้อ 7 เมื่อพนักงานมีการเปลี่ยนชื่อ-นามสกุล เปลี่ยนตำแหน่งงาน โอนย้าย ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่แก้ไขข้อมูลบัญชีของผู้ใช้งานให้ถูกต้อง หรือปิดบัญชีผู้ใช้งานเมื่อพนักงานลาออก

- **การใช้ระบบเทคโนโลยีสารสนเทศจากภายนอกสำนักงาน**

สิทธิ์การเข้าใช้งานระบบเทคโนโลยีสารสนเทศจากภายนอกสำนักงาน ต้องเป็นผู้ที่มีความจำเป็นต้องใช้งาน และต้องได้รับอนุมัติจากต้นสังกัดและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ โดยมีข้อปฏิบัติ ดังนี้

ข้อ 1 การเข้าใช้ระบบเทคโนโลยีสารสนเทศจากภายนอกสถานที่ทำการของบริษัท ต้องใช้วิธี Virtual Private Network, VPN ที่ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ติดตั้งโปรแกรมให้เท่านั้น

ข้อ 2 ผู้ใช้ ต้องใช้ชื่อบัญชีและรหัสผ่านส่วนบุคคลของตนเอง ในการยืนยันตัวตนทุกครั้ง

ข้อ 3 เมื่อสิ้นสุดการทำงาน ผู้ใช้ต้องทำการปิด VPN โดยทันที

ข้อ 4 กรณีใช้เครือข่ายสาธารณะ ผู้ใช้ต้องตรวจสอบว่าเครือข่ายสาธารณะที่ใช้นั้นเป็นเครือข่ายที่น่าเชื่อถือ และตรวจสอบว่าโปรแกรมตรวจสอบไวรัสคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของตนเองยังทำงานได้ตามปกติ ให้หลีกเลี่ยงการ Download โปรแกรมต่างๆ เนื่องจากอาจเป็นโปรแกรมไวรัสคอมพิวเตอร์ ถ้าพบว่าคอมพิวเตอร์ทำงานผิดปกติระหว่างการใช้เครือข่ายสาธารณะ ให้ปิดเครื่องคอมพิวเตอร์ทันที และส่งคอมพิวเตอร์ให้ฝ่ายเทคโนโลยีสารสนเทศตรวจสอบและแก้ไขปัญหาต่อไป

นโยบายการป้องกันข้อมูลสารสนเทศ

การใช้ข้อมูลและทรัพยากรเทคโนโลยีสารสนเทศของบริษัท พนักงานต้องใช้ชื่อบัญชีผู้ใช้งาน และรหัสผ่านส่วนบุคคลของตนเอง เพื่อยืนยันตัวบุคคล พนักงานต้องไม่ใช้ทรัพยากรเทคโนโลยีสารสนเทศเพื่อวัตถุประสงค์ดังต่อไปนี้

ข้อ 1 เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

ข้อ 2 เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

ข้อ 3 เพื่อการพาณิชย์

ข้อ 4 เพื่อเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งของบริษัทหรือบุคคลภายนอกก็ตาม

ข้อ 5 เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กรหรือของบุคคลอื่น

ข้อ 6 เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิ์ในข้อมูล

ข้อ 7 เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่บริษัท เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายแบบลูกโซ่ หรือแบบกระจาย หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังพนักงานหรือบุคคลอื่น เป็นต้น

ข้อ 8 เพื่อขัดขวางการใช้งานเครือข่ายเทคโนโลยีสารสนเทศของบริษัท หรือของพนักงาน หรือเพื่อให้เครือข่ายเทคโนโลยีสารสนเทศของบริษัท ไม่สามารถใช้งานได้ตามปกติ

ข้อ 9 เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของบริษัท ไปยังสื่อสังคมออนไลน์ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

ข้อ 10 เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ของบริษัท หรืออาจก่อให้เกิดความขัดแย้ง หรือก่อให้เกิดความเสียหายแก่บริษัท

ขั้นตอนในการปฏิบัติเพื่อความปลอดภัยในระบบเทคโนโลยีสารสนเทศ

เพื่อความปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศ พนักงานมีหน้าที่ต้องปฏิบัติ ดังต่อไปนี้

ข้อ 1 ไม่ติดตั้งหรือใช้โปรแกรมคอมพิวเตอร์ที่เป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

ข้อ 2 ไม่ติดตั้งหรือใช้โปรแกรมคอมพิวเตอร์ที่สามารถตรวจสอบข้อมูลบนเครือข่ายเทคโนโลยีสารสนเทศ เว้นแต่จะได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ข้อ 3 ไม่ติดตั้งหรือใช้โปรแกรมคอมพิวเตอร์ เพื่อให้บุคคลอื่นสามารถใช้เครื่องคอมพิวเตอร์ส่วนบุคคลของตนเองหรือผู้อื่น หรือให้ใช้ระบบเครือข่ายเทคโนโลยีสารสนเทศของบริษัทได้ เว้นแต่จะได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

ข้อ 4 ปิดเครื่องคอมพิวเตอร์ของตนเอง เมื่อสิ้นสุดการทำงานในแต่ละวัน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องที่มีการให้บริการแบบ Server

ข้อ 5 ตรวจสอบข้อมูลที่ได้รับจากบุคคลภายนอกทุกครั้งด้วยโปรแกรมคอมพิวเตอร์ที่ใช้สำหรับการตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ตามที่ฝ่ายเทคโนโลนีสารสนเทศกำหนด และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด หรือแจ้งฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ

ข้อ 6 การใช้เครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการของบริษัท ให้ใช้โปรแกรมคอมพิวเตอร์ที่ฝ่ายเทคโนโลยีเป็นผู้กำหนดเท่านั้น

ข้อ 7 ให้ความร่วมมือและอำนวยความสะดวกแก่ฝ่ายเทคโนโลยีสารสนเทศในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล รวมทั้งปฏิบัติตามคำแนะนำจากฝ่ายเทคโนโลยีสารสนเทศ

ข้อ 8 ระมัดระวังการใช้งานและรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายเทคโนโลยีสารสนเทศให้พร้อมใช้งานได้ตลอดเวลา

ข้อ 9 พึงระมัดระวังและเก็บรักษาข้อมูลของบริษัทไว้อย่างมั่นคงและปลอดภัย

ข้อ 10 การส่งข้อมูลที่มีความสำคัญของบริษัท ให้พึงระมัดระวังความปลอดภัยของข้อมูลไว้สูงสุด

ข้อ 11 การพิมพ์หรือการทำสำเนาเอกสาร ให้พึงระมัดระวังและรักษาความลับของข้อมูล และควรจัดเก็บข้อมูลไว้ในสถานที่ที่มีการจัดเก็บอย่างปลอดภัย

ข้อ 12 ก่อนการส่งซ่อมคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลให้ฝ่ายเทคโนโลยีสารสนเทศ พนักงานต้องทำการสำรองข้อมูลทั้งหมดที่มีอยู่และจัดเก็บไว้ในที่ปลอดภัย เพื่อป้องกันข้อมูลสูญหาย

ข้อ 13 คืนทรัพย์สินทั้งหมดของบริษัท ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น เครื่องคอมพิวเตอร์ ข้อมูล สำเนาของข้อมูล ก่อนวันพ้นสภาพการเป็นพนักงาน

ข้อ 14 ห้ามเข้าห้อง Data Center ก่อนได้รับการอนุมัติ

ระเบียบการใช้ Internet และ Email

การใช้ Internet ให้มีความปลอดภัย พนักงานต้องปฏิบัติ ดังต่อไปนี้

- Internet

ข้อ 1 ใช้ Internet โดยใช้ชื่อบัญชีของตนเองเท่านั้น

ข้อ 2 ใช้ Internet ในส่วนที่เกี่ยวข้องกับการปฏิบัติงานเท่านั้น

ข้อ 3 ไม่ Download โปรแกรม เกมส์ รูปภาพ หรือข้อมูลอื่นใดที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

ข้อ 4 ไม่เปิดรูปภาพ ภาพเคลื่อนไหว หรือข้อความที่สื่อไปในทางลามกอนาจาร หรือเป็นสิ่งที่ขัดต่อศีลธรรมอันดี

ข้อ 5 ไม่เล่นเกมส์ Online หรือใช้บริการอื่นๆที่เกี่ยวข้องกับเกมส์

ข้อ 6 ไม่ส่งรูปภาพ ภาพเคลื่อนไหว ข้อความ หรือข้อมูลในรูปแบบใดๆ ที่ก่อให้เกิดความเสื่อมเสียกับบริษัท สถาบันอันเป็นที่เคารพ ศาสนา องค์กร หรือบุคคลที่สาม

- Email

ข้อ 1 ใช้ Email โดยใช้ชื่อบัญชีของตนเองเท่านั้น

ข้อ 2 ใช้ Email ของบริษัท ในส่วนที่เกี่ยวข้องกับการปฏิบัติงานเท่านั้น

ข้อ 3 ห้าม เปิดเผยรหัสผ่านส่วนบุคคลของตนเองให้แก่ผู้อื่นรับทราบ

ข้อ 4 ห้าม ส่ง Email แบบลูกโซ่ หรือแบบกระจายที่ไม่เกี่ยวกับการปฏิบัติงาน

ข้อ 5 การรับ Email ที่มีการแนบเอกสาร ต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนเปิดเอกสารทุกครั้ง

นโยบายการบริหารและการป้องกันระบบเทคโนโลยีสารสนเทศ

ความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นสิ่งที่สำคัญของบริษัท เพื่อให้การใช้ระบบสารสนเทศเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ ลดความเสี่ยงที่อาจจะเกิดขึ้นจากการปฏิบัติงาน อีกทั้งเป็นการบริหารระบบเครือข่ายเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ จึงกำหนดข้อปฏิบัติ ดังต่อไปนี้

- **การสำรองข้อมูล**

หน้าที่หลักของ ระบบสำรองข้อมูล คือการจัดเก็บสำเนาข้อมูลที่มีอยู่ลงในสื่อบันทึกข้อมูล เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นจากการเข้าทำลายข้อมูลจากผู้ไม่หวังดี รวมถึงมีวิธีการกู้คืนข้อมูลให้กลับมาได้ตามเดิม โดยมีวิธีการปฏิบัติดังนี้

ข้อ 1 ผู้ที่ดำเนินการจัดเก็บสำเนาข้อมูล และการกำหนดสถานที่ของการจัดเก็บข้อมูลสำรองไว้ในที่ปลอดภัย ต้องเป็นผู้ที่ได้รับมอบหมายและได้รับอนุมัติจากผู้บังคับบัญชาต้นสังกัดเท่านั้น

ข้อ 2 ผู้รับผิดชอบ ต้องทำการสำรองข้อมูลและเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูล

ข้อ 3 สถานที่เก็บสำรองข้อมูล ประกอบด้วย แบบภายในบริษัทและแบบภายนอกบริษัท กรณี สถานที่เก็บข้อมูลแบบภายนอกของสำนักงานใหญ่ หมายถึง การสำรองข้อมูลไปที่ศูนย์คอมพิวเตอร์สำรอง

ข้อ 4 ในการเคลื่อนย้าย หรือเปลี่ยนสถานที่จัดเก็บข้อมูลสำรอง จะต้องมีการแจ้งอย่างเป็นลายลักษณ์อักษร โดยผู้ปฏิบัติจะต้องได้รับการอนุมัติจากผู้บังคับบัญชาต้นสังกัดก่อน

ข้อ 5 ผู้รับผิดชอบต้องสามารถนำสื่อบันทึกข้อมูลที่ได้สำรองไว้ จากสถานที่จัดเก็บได้ทันที และสามารถกู้คืนระบบได้ภายในระยะเวลาอย่างรวดเร็ว หากเกิดเหตุการณ์ที่ไม่คาดคิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

- **การรายงานสถานะของระบบเครือข่ายเทคโนโลยีสารสนเทศ**

วัตถุประสงค์ของของการรายงานสถานะของระบบเครือข่ายเทคโนโลยีสารสนเทศ มีดังนี้

ข้อ 1 ตรวจสอบและติดตามผลการใช้ระบบเครือข่ายเทคโนโลยีสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ข้อ 2 ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ ต้องจัดเก็บประวัติข้อมูลของ Internet Traffic, Email Traffic และข้อมูลจากระบบอื่นๆ เช่น System Error, Backup & Recovery, Anti-Virus, Wireless Network เป็นต้น

ข้อ 3 ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ ต้องตรวจสอบการบุกรุก ตรวจสอบสิทธิการเข้าถึงระบบ ตรวจสอบการเดาสุ่มรหัสผ่าน ตรวจสอบการใช้ข้อมูลร่วมกัน

ข้อ 4 ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ ต้องบำรุงรักษาและตรวจสอบระบบการทำงานต่างๆของห้อง Data Center และศูนย์คอมพิวเตอร์สำรอง ให้สามารถใช้งานได้ตามปกติอย่างสม่ำเสมอ

ข้อ 5 ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ มีหน้าที่รายงานสถานะของระบบเครือข่ายเทคโนโลยีสารสนเทศในที่ประชุมฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้พนักงานของฝ่ายเทคโนโลยีสารสนเทศทราบถึงความเสี่ยงและแนวโน้มของภัยคุกคามที่เกิดขึ้น เพื่อร่วมกันแก้ไขปัญหาและกำหนดมาตรการป้องกันภัยคุกคามนั้น

- **การป้องกันการบุกรุกและการป้องกันการแพร่กระจายของไวรัสคอมพิวเตอร์**

บริษัทมีอุปกรณ์ป้องกันความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เหมาะสม โดยผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ มีหน้าที่ดังนี้

ข้อ 1 ติดตั้ง Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีที่พยายามเข้าระบบเครือข่ายเทคโนโลยีสารสนเทศ

ข้อ 2 ปรับปรุงเวอร์ชั่นของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ให้ทุกเครื่องมีความทันสมัยอยู่ตลอดเวลา

ข้อ 3 มีการตรวจสอบไวรัสคอมพิวเตอร์จากการรับส่ง Email ทุกฉบับ

ข้อ 4 ปิดช่องโหว่ของระบบปฏิบัติการคอมพิวเตอร์ โดยการอัพเดตแพทช์ให้มีความทันสมัยอย่างสม่ำเสมอ

ข้อ 5 ป้องกันการแพร่กระจายของไวรัสคอมพิวเตอร์ จากเครื่องคอมพิวเตอร์ที่ติดไวรัส โดยการตัดการเชื่อมต่อของคอมพิวเตอร์นั้นออกจากระบบเครือข่ายเทคโนโลยีสารสนเทศก่อน แล้วจึงกำจัดไวรัสให้เรียบร้อยต่อไป

- **การให้บริการ การรักษาความปลอดภัยและการควบคุมอุปกรณ์คอมพิวเตอร์**

ข้อ 1 กำหนดให้มีรหัสผ่านส่วนบุคคล เพื่อป้องกันการรั่วไหลและความเสียหายของข้อมูลที่อาจจะเกิดขึ้น

ข้อ 2 ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ควบคุมอุปกรณ์เทคโนโลยีสารสนเทศของบริษัท ให้มีความเหมาะสมกับการใช้งานของแต่ละส่วนงาน

ข้อ 3 การจัดซื้ออุปกรณ์เทคโนโลยีสารสนเทศ ให้ผ่านขั้นตอนการจัดซื้อของบริษัท โดยต้องได้รับอนุมัติจากผู้บังคับบัญชาต้นสังกัดก่อน

ข้อ 4 ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่ขึ้นทะเบียนทรัพย์สินเมื่อได้รับของจากผู้จำหน่าย โดยการกำหนดหมายเลขประจำเครื่อง และรายละเอียดอื่นๆที่จำเป็นตามแต่ละประเภทของอุปกรณ์

ข้อ 5 การโอนย้ายสถานที่ที่ใช้งานอุปกรณ์เทคโนโลยีสารสนเทศ ต้องได้รับการอนุมัติจากผู้บังคับบัญชาต้นสังกัด

ข้อ 6 ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่สนับสนุนการทำงานและซ่อมบำรุงอุปกรณ์เทคโนโลยีสารสนเทศ ตามคำร้องขอจากผู้ใช้บริการ โดยต้องดำเนินการอย่างรวดเร็วและเหมาะสม และจัดเก็บประวัติการซ่อมบำรุงทุกครั้ง

ข้อ 7 การให้บริการของฝ่ายเทคโนโลยีสารสนเทศแบบระยะไกล เป็นกรณีที่จำเป็นต้องเข้าถึงเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานผู้ขอรับบริการอย่างทันที โดยพนักงานต้องยินยอมการรับบริการดังกล่าวบนเครื่องคอมพิวเตอร์ของตนเองก่อนจึงจะให้บริการแบบระยะไกลได้ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลและป้องกันการสูญหายของข้อมูล

ข้อ 8 การตัดจำหน่ายอุปกรณ์เทคโนโลยีสารสนเทศ ต้องได้รับการอนุมัติจากประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

ข้อ 9 กรณีพนักงานมีการติดตั้งหรือใช้โปรแกรมคอมพิวเตอร์ที่เป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาบนเครื่องคอมพิวเตอร์ของบริษัท หรือมีการใช้โปรแกรมคอมพิวเตอร์ที่เป็นการละเมิดสิทธิบนคอมพิวเตอร์ส่วนบุคคลของตนเอง ผู้ที่ละเมิดต้องเป็นผู้รับผิดชอบเป็นการส่วนตัวที่ได้กระทำการอันเป็นความผิดตามกฎหมาย

- **การรักษาความปลอดภัยของข้อมูลและการพัฒนาโปรแกรมตามมาตรฐานสากล**

แนวทางการพัฒนาโปรแกรมต้องมีความมั่นคงและทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี โดยโปรแกรมที่พัฒนานั้นจะมีการออกแบบให้ไม่สามารถถูกโจมตีได้ด้วยเครื่องมือที่เป็นที่นิยมใช้กันอย่างแพร่หลาย เช่น ภัยคุกคามแบบปฏิเสธการให้บริการ (Denial of Service), ภัยคุกคามแบบการปลอมตัว (Spoofing), Malware, Ransomware, Phishing เป็นต้น

ข้อกำหนด การพัฒนาโปรแกรมให้มีความมั่นคงปลอดภัยของข้อมูล มีดังนี้

ข้อ 1 การตรวจสอบช่องโหว่ของความปลอดภัยของโปรแกรม

ข้อ 2 การพิสูจน์และยืนตัวตน

ข้อ 3 การกำหนดสิทธิ์ในการเข้าถึงข้อมูล

ข้อ 4 การบันทึกประวัติการเข้าใช้โปรแกรม การบันทึกประวัติการใช้รหัสผ่านที่ไม่ถูกต้อง

ข้อ 5 การทดสอบการถูกโจมตีฐานข้อมูลแบบ SQL Injection

ข้อ 6 การกำหนดจำนวนครั้งที่รหัสผ่านไม่ถูกต้อง หรือใช้วิธีการยืนยันตัวแบบหลายปัจจัย เพื่อป้องกันการโจมตีแบบปฏิเสธการให้บริการ

ข้อ 7 การปกป้องข้อมูลเมื่อมีการรับส่งข้อมูล โดยการเข้ารหัสข้อมูล เพื่อป้องกันการโจมตีแบบปลอมตัว

ข้อกำหนด การพัฒนาโปรแกรมตามมาตรฐานสากล มีดังนี้

ข้อ 1 ผู้พัฒนาโปรแกรม ต้องพัฒนาโปรแกรมตามรูปแบบมาตรฐานเป็นที่ยอมรับโดยทั่วไป รวมทั้งแสดงรายละเอียดต่างๆที่จำเป็นต่อการรักษาความปลอดภัย และมี Source Code ของโปรแกรม คู่มือประกอบการพัฒนา คู่มือการใช้งานของผู้ใช้ รวมถึงข้อมูลต่างๆที่จำเป็นในการพัฒนา เช่น ความสัมพันธ์ที่สามารถเชื่อมโยงไปยังโปรแกรมหรือข้อมูลอื่นๆ เป็นต้น

ข้อ 2 ผู้บังคับบัญชาต้นสังกัด เป็นผู้พิจารณาและกำหนดคุณสมบัติของผู้ที่สามารถใช้โปรแกรม และกำหนดสิทธิ์ต่างๆให้แต่ละผู้ใช้งาน

ข้อ 3 โปรแกรมที่พัฒนาขึ้นต้องได้รับการทดสอบความถูกต้องในการทำงานของโปรแกรมก่อนส่งมอบให้ผู้ใช้ และผู้ใช้ต้องตรวจสอบความถูกต้องของโปรแกรมพร้อมลงนามรับงาน

ข้อ 4 การพัฒนาโปรแกรมที่ต้องเข้าถึงฐานข้อมูลส่วนกลาง จะต้องทำบนฐานข้อมูลทดสอบโดยหลีกเลี่ยงการทำงานบนฐานข้อมูลหลัก เพื่อป้องกันข้อผิดพลาดและรักษาความปลอดภัยของข้อมูล

ข้อ 5 โปรแกรมที่ได้รับการพัฒนาที่จำเป็นต้องติดตั้งและใช้งานบนระบบเครือข่าย ผู้ดำเนินการติดตั้งคือผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศ ส่วนการติดตั้งใช้งานเฉพาะส่วนให้ดำเนินการโดยเจ้าหน้าที่บริการเทคโนโลยีสารสนเทศ

ข้อ 6 กรณีผู้พัฒนาโปรแกรมมีความจำเป็นต้องเข้าแก้ไขโปรแกรมที่ใช้บนระบบเครือข่ายเทคโนโลยีสารสนเทศ ให้ผู้ดูแลระบบเครือข่ายเทคโนโลยีสารสนเทศเปิดสิทธิ์ให้กับผู้พัฒนาโปรแกรมเป็นกรณีๆไป และควบคุมการเข้าใช้งานของผู้พัฒนาโปรแกรมจนแล้วเสร็จ

นโยบายการป้องกันและกู้คืนระบบเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยและสามารถกู้คืนระบบเทคโนโลยีสารสนเทศได้อย่างรวดเร็ว ตามมาตรฐานสากล อีกทั้งเป็นการป้องกันปัญหาที่อาจก่อหรือก่อให้เกิดกับข้อมูลหรือระบบงานอันเนื่องจากข้อผิดพลาดหรือความเสียหายจากภัยต่างๆ

สำหรับระบบเทคโนโลยีสารสนเทศของสำนักงานใหญ่ ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการสำรองข้อมูลและระบบงานทั้งหมดไปยังศูนย์คอมพิวเตอร์สำรอง กำหนดวิธีการกู้คืนข้อมูลและวิธีการกู้คืนระบบงานทั้งหมด การทดสอบการกู้คืนข้อมูลและกู้คืนระบบงานที่มีความสำคัญ เพื่อป้องกันไม่ให้มีผลกระทบต่อการดำเนินกิจการของบริษัทอย่างมีนัยสำคัญ โดยวิธีการสำรองข้อมูลและวิธีการกู้คืนข้อมูล ให้เป็นไปตามแนวทางปฏิบัติเรื่อง การสำรองข้อมูลและกู้คืนข้อมูล

ข้อปฏิบัติของผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ

ข้อ 1 ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ ต้องดูแลรักษาและปรับปรุงระบบเครือข่ายระบบเทคโนโลยีสารสนเทศให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งต้องมีการประเมินความเสี่ยงจากภัยคุกคามใหม่ๆ มีการตรวจสอบการใช้เครือข่ายระบบเทคโนโลยีสารสนเทศ เพื่อให้ใช้เครือข่ายระบบเทคโนโลยีสารสนเทศเป็นไปตามนโยบายนี้อย่างเคร่งครัด หากผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศพบว่าพนักงานผู้ใดมี

พฤติการณ์ต่อไปในทางที่จะละเมิดข้อกำหนดการใช้งาน ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศต้องแจ้งให้ผู้บังคับบัญชาต้นสังกัดทราบโดยเร็วที่สุด

ข้อ 2 หากพบว่าเหตุที่เกิดขึ้นอาจมีผลก่อให้เกิดความเสียหายขึ้นกับบริษัท ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศมีอำนาจระงับการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศของพนักงานดังกล่าวได้ทันที

ข้อ 3 ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ มีหน้าที่ในการเสนอความคิดเห็นและข้อสังเกตต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เพื่อปรับปรุงประสิทธิภาพและการบริหารเครือข่ายระบบเทคโนโลยีสารสนเทศ

ข้อ 4 ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ มีหน้าที่ติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศ ระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายระบบเทคโนโลยีสารสนเทศ ตลอดจนการบำรุงรักษาให้ใช้งานได้ดีอยู่เสมอ

ข้อ 5 ผู้ดูแลเครือข่ายระบบเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนให้แก่ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เมื่อพ้นจากหน้าที่เพื่อความปลอดภัยของข้อมูลและเครือข่ายระบบเทคโนโลยีสารสนเทศ

<u>บทลงโทษและการบังคับใช้</u>

ข้อ 1 พนักงานที่ฝ่าฝืนนโยบายนี้ บริษัทจะดำเนินการทางวินัยและกฎหมายตามระเบียบกฎเกณฑ์ของบริษัท

ข้อ 2 ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ดูแลการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ 3 นโยบายนี้ได้รับการอนุมัติจากคณะกรรมการบริษัท ครั้งที่ 2/2567 เมื่อวันที่ 27 กุมภาพันธ์ 2567 และให้มีผลใช้บังคับตั้งแต่วันที่ 27 กุมภาพันธ์ 2567 เป็นต้นไป

ประกาศใช้ วันที่ 27 กุมภาพันธ์ 2567

ลงชื่อ .....

(นายวัลลภ รุ่งกิจวรเสถียร)

ประธานกรรมการบริษัท

บริษัท สเตคอน กรุ๊ป จำกัด (มหาชน)