นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (สำหรับผู้ดูแลระบบ)

(ฉบับปรับปรุง 23 มกราคม 2566)

วัตถุประสงค์

เพื่อให้ผู้ดูแลระบบและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งรับทราบหน้าที่และความรับผิดชอบและใช้เป็นแนวทางในการปฏิบัติงานและการควบคุมด้านต่างๆ โดยมีแนวทางปฏิบัติดังนี้

1. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties)

1.1 จัดให้มีการกำหนดบุคลากรเจ้าหน้าที่ IT ดูแลและบริหารระบบเทคโนโลยีสารสนเทศ (IT System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง

1.2 จัดให้มีเอกสารคำบรรยายลักษณะงาน (Job Description) ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคน

2. การควบคุมการเข้าออกห้อง Server

2.1 มีการติดตั้งระบบกล้องวงจรปิดภายในห้องควบคุมระบบและเครือข่าย เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหาย อื่นๆที่อาจเกิดขึ้นได้

2.2 จัดให้มีการจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น Active Directory Server, ERP Server, Mobile Server, File Server, Stock Server, TigerSoft Server, Maintenance Server, Router, Switch Hub เป็นต้น ไว้ในห้อง Server ซึ่งอนุญาตให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ IT สามารถเข้าไปในห้อง Server ได้เท่านั้น

2.3 มีระบบ Access Control ในการควบคุมผู้ที่มีสิทธิ์ในการเข้าห้อง Server

3. การควบคุมการเข้าถึงข้อมูล

3.1 จัดให้มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียด เกี่ยวกับเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

3.2 แบ่งกลุ่มผู้ใช้งานตามระดับตำแหน่งและฟังชั่นการงานต่างๆให้มีความเหมาะสม เพื่อจำกัดสิทธิการใช้งานของผู้ใช้งานแต่ละกลุ่มให้สอดคล้องตามความจำเป็น

3.3 กำหนดให้เจ้าหน้าที่ IT เป็นผู้มีสิทธิในการเปลี่ยนแปลง แก้ไข เพิ่ม-ลด จำนวนผู้ใช้งานของแต่ละโปรแกรมที่สำคัญๆ รวมถึงผู้ใช้งาน E-mail

3.4 ไม่อนุญาตให้ผู้ใช้งานติดตั้งระบบปฏิบัติการและโปรแกรมต่างๆโดยพละการเพื่อป้องกันการใช้งานระบบปฏิบัติการและโปรแกรมที่ละเมิดลิขสิทธิ์ การติดตั้งโปรแกรมต่างๆ ต้องทำโดยเจ้าหน้าที่ IT เท่านั้นซึ่งจะควบคุมผ่าน User ผู้ดูแลระบบ

4. การป้องกันความเสียหายของข้อมูล

4.1 ระบบป้องกันไฟไหม้

4.1.1 จัดให้มีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา รวมถึงจัดให้มีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

4.1.2 มีการกำจัดวัสดุที่สามารถติดไฟออกจากห้อง Server อย่างสม่ำเสมอเพื่อลดความเสี่ยงจากเกิดอัคคีภัย

4.2 ระบบป้องกันไฟฟ้าขัดข้อง

จัดให้มีระบบไฟสำรองเพื่อป้องกันมิให้อุปกรณ์เครือข่ายและชุด Server ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ อีกทั้งเพื่อให้ Server สามารถทำงานได้อย่างต่อเนื่องประมาณ 20-30 นาที ซึ่งเพียงพอต่อการให้ผู้ดูแลระบบสามารถ Shut Down ชุด Server ได้ทัน เพื่อป้องกันความเสียหายกับข้อมูล และ Hardware ต่างๆ

4.3 ระบบควบคุมอุณหภูมิและความชื้น

จัดให้มีการควบคุมสภาพแวดล้อมที่เหมาะสมกับคุณลักษณะ (Specification) ของ Server โดยจัดให้มีระบบปรับอากาศ พร้อมทั้งระบบสลับการทำงานเครื่องปรับอากาศ 2 ชุด เพื่อให้มั่นใจว่าอุณหภูมิของเครื่อง Server จะต้องไม่สูงเกิน 25 องศาเซลเซียส และมีเครื่องปรับอากาศสำรองหากเครื่องปรับอากาศตัวใดตัวหนึ่งไม่ทำงาน

4.4 อุปกรณ์ดับเพลิง

จัดให้มีถังดับเพลิงติดตั้งไว้ใกล้ห้อง Server และมีการตรวจสอบอุปกรณ์ทุกๆ 6 เดือน

4.5 ระบบ Server (ระบบ HCI) และ Firewall

จัดให้มีชุดอุปกรณ์ Server & Firewall มากกว่า 1 ชุด ซึ่ง Hardware รองรับการทำงานแบบ Main และ Mirror เมื่อเครื่องใดเครื่องหนึ่งเกิดความเสียเสียหาย ระบบจะ switch การทำงานไปยังอีกเครื่องโดยอัตโนมัติ อีกทั้งสภาวะการทำงานปกติชุดอุปกรณ์ทั้งสองยังร่วมกันประมวลผลและทำงานร่วมกันเพื่อใช้งานทรัพยากรได้อย่างมีประสิทธิภาพ

5. ระบบป้องกัน ไวรัสคอมพิวเตอร์/ การทำลาย/ การสำเนา/ หรือการเข้าถึงข้อมูลโดยมิชอบ

5.1 เครื่อง Server และ Client ได้ติดตั้งซอฟต์แวร์ Antivirus ทุกเครื่อง และได้รับการ update ฐานข้อมูลไวรัส แบบ Real Time เพื่อป้องกันไวรัสคอมพิวเตอร์ได้อย่างทันท่วงที

5.2 จัดให้มีระบบกำแพงเสมือน (Firewall: Sangfor) แบบ Hardware เพิ่มเติมนอกเหนือจากแบบ Software เพื่อป้องกันบุคคลภายนอก ไวรัส และ Ransomware เข้าถึงเครือข่ายคอมพิวเตอร์ภายในโดยมิชอบ

5.3 ที่ประตูเข้าออก (Gateway) ระหว่างเครือข่ายคอมพิวเตอร์ภายในองค์กร (LAN) และเครือข่ายอินเตอร์เน็ตภายนอกองค์กร (WAN) ได้ติดตั้งกำแพงไฟเสมือน เพื่อป้องกันบุคคลภายนอกเข้าถึงเครือข่ายคอมพิวเตอร์ภายในโดยมิชอบ

6. การสำรองข้อมูล และการเตรียมพร้อมกรณีฉุกเฉิน

6.1 จัดให้มีการสำรองข้อมูลแบบถี่ทุกๆ 15 วินาที (CDP) สำหรับระบบ ERP (Web service & DB Service)/ MOBILE APP (Web service & DB Service)/ ALFRESCO (Web service & DB Service)/ STOCK และสำรองข้อมูลแบบถี่ทุกๆ 60 นาที สำหรับระบบ Active Directory (AD) ทำให้สามารถเรียกคืนข้อมูลกลับคืนได้ไม่ต่างจากสภาวะการทำงานเวลาขณะนั้น (ระบบอื่นๆ สำรองข้อมูลทุกสิ้นวันทำงาน เช่น Tiger Soft/ EXPRESS/ Maintenance)

6.2 จัดให้มีการทดลองการ Recovery data ทุก ๆ 6 เดือน เพื่อให้มั่นใจว่าการ Backup เป็นไปอย่างถูกต้องสมบูรณ์นอกจากนี้ ยังมีการทำ Replication ของตัว Server เพื่อที่จะสำรองข้อมูลในกรณี Hard disk ของ Server ลูกใดลูกนึ่งมีปัญหา จะสามารถใช้งานข้อมูลจาก Server อีกตัวได้ ซึ่งในกรณีที่มีเหตุฉุกเฉิน ผู้ใช้สามารถแจ้งทางเจ้าหน้าที่ IT เพื่อตรวจสอบ และ Recovery ข้อมูลเพื่อให้สามารถทำงานต่อได้

6.3 จัดให้มีระบบเก็บสำรองข้อมูลใน NAS (1st Backup) ณ สำนักงานใหญ่ เพิ่มเติมนอกเหนือจากระบบ HCI ที่สามารถเรียกคืนข้อมูลได้

6.4 จัดให้มีศูนย์เก็บสำรองข้อมูลแบบ Cloud (2nd Backup) ณ โรงงานลาดหลุมแก้ว เพื่อรองรับภัยพิบัติฉุกเฉิน (Disaster Recovery) อันไม่สามารถเข้าถึงกับศูนย์ข้อมูลกลางของสำนักงานใหญ่ได้ โดยการสำเนาข้อมูลจาก NAS (1st Backup) มาจัดเก็บในศูนย์ข้อมูลดังกล่าวภายนอกสำนักงานใหญ่เพื่อป้องกันกรณีฉุกเฉินที่อาจเกิดผลกระทบทั้งชุด Main server และ Mirror server เสียหายไม่สามารถทำงานได้

6.5 จัดให้มีการซักซ้อมการเรียกคืนระบบเมื่อเกิดเหตุฉุกเฉินทุกๆ 6 เดือน เช่น กรณีถูกโจมตีจากไวรัส/ Ransomware/ ข้อมูลบางส่วนสูญหาย/ และชุด Server/ Firewall ของระบบ HCI เสียหาย 1 ชุด

6.6 จัดให้มีแผนฉุกเฉินเมื่อเกิดภัยพิบัติต่อการเข้าถึงระบบเทคโนโลยีสารสนเทศ ณ สำนักงานใหญ่ เช่น อัคคีภัย อุทกภัย สถานการณ์โรคและภัยต่อสุขภาพ

7. การใช้จดหมายอิเล็กทรอนิกส์ (E-mail)

7.1 กำหนดให้มีผู้ดูแลระบบอีเมล์ชัดเจนและมีบัญชีผู้ดูแลระบบจำแนกรายคน

7.2 กำหนดให้มีการเก็บบันทึกประวัติการใช้งาน Email ย้อนหลัง 15วัน

7.3 ตรวจสอบสิทธิ์และลบสิทธิ์การใช้งาน Email ของพนักงานที่ลาออก ทุกเดือน

8. การรักษาความปลอดภัยในการใช้งานอินเตอร์เน็ต ผ่านระบบ Firewall: Sangfor

8.1 กำหนดให้มีการเก็บบันทึกประวัติการใช้งานอินเตอร์เน็ตย้อนหลังไม่น้อยกว่า 90วัน

8.2 ทำการตรวจสอบการใช้งานอินเตอร์เน็ตของพนักงานในองค์กรทุกเดือน

8.3 ตรวจสอบสิทธิ์และลบสิทธิ์การใช้งาน Internet ผ่านระบบ Lan และ Wifi ของพนักงานที่ลาออกทุกเดือน

8.4 กำหนดให้มีการตรวจสอบความผิดปรกติการเข้าถึงจากผู้บุกรุก/ บุคคลภายนอกทุกสัปดาห์และกำหนดมาตรการแก้ไขตามความเหมาะสม

9. การรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์ จากระบบเครือข่ายส่วนกลาง (Active Directory Server)

9.1 กำหนดให้เครื่องคอมพิวเตอร์ ต้องทำการเชื่อมต่อกับระบบเครือข่ายส่วนกลางในแบบ Active Directory

หมายเหตุ ถ้าเครื่องคอมพิวเตอร์ ไม่สามารถเชื่อมต่อ Active Directory ได้ เครื่องนั้นจะต้องถูกจำกัดสิทธิ์การใช้งานเครื่องในระดับ user ของคอมพิวเตอร์เท่านั้น

9.2 กำหนดให้ผู้ใช้งานเปลี่ยน Password สำหรับ Login ทุกๆ 90 วัน โดยใช้การตั้งค่าไว้ที่ Domain ของบริษัท ทั้งนี้ รูปแบบ Password ต้องความยาวเกิน 8 ตัวอักษรและประกอบด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่, ตัวเลข และสัญลักษณ์อย่างน้อยอย่างละ 1 ตัว

9.3 กำหนดให้ระบบ Log-off ออกอัตโนมัติเมื่อผู้ใช้งานไม่มีการใช้งานต่อเนื่องกัน 10 นาที โดยใช้การตั้งค่าไว้ที่ระบบ Domain ของบริษัท

9.4 ทำการตรวจสอบเครื่องคอมพิวเตอร์และโน๊ตบุ๊คว่าพนักงานสามารถติดตั้งโปรแกรมได้ด้วยตัวเองหรือไม่ โดยทำการตรวจสอบทุกๆ 6 เดือน

9.5 จัดให้มีการเปลี่ยน Password ของระบบ Active Directory, ERP, Alfresco, Express, TigerSoft, Stock ทุกๆ 6 เดือน

10. นโยบายด้านอื่นๆ

10.1 จัดให้มีการประเมินความเสี่ยงด้านสารสนเทศในด้านต่างๆ เช่น การถูกโจมตีทางไซเบอร์ระบบเครือข่ายส่วนกลาง เป็นต้น โดยผู้บริหารของบริษัทเป็นประจำทุกไตรมาส

10.2 มีการประกาศและเผยแพร่พรบ. ที่เกี่ยวข้องกับการกระทำผิดคอมพิวเตอร์และเทคโนโลยีสารสนเทศให้กับพนักงานในบริษัทรับทราบ

10.3 มีการแยกวง LAN สำหรับการเชื่อมต่อ Internet ของผู้ที่เข้ามาติดต่อเพื่อจำกัดสิทธิและเวลาใช้งานของบุคคลภายนอก

10.4 กำหนดให้มีระบบ service ticket เพื่อใช้ในการขอรับบริการต่างๆ ด้านเทคโนโลยีสารสนเทศจากทีมไอที

10.5 จัดให้มีระบบบันทึกการโยกย้ายทรัพย์สินไอที เพื่อติดตามการใช้งานจากผู้ใช้จากสถานที่ต่างๆ

10.6 จัดให้มีระบบ KNOX/ WeGuard ติดตามและควบคุมการใช้งานอุปกรณ์สมาร์ทโฟนและแทบเล็ต เพื่อที่จะป้องกันอุปกรณ์และข้อมูลทำงานของบริษัทสูญหาย

10.7 กำหนดให้ระบบกล้องวงจรปิด CCTV มีการเก็บ Log ย้อนหลังอย่างน้อย 30 วัน และจัดให้มีผู้ดูแลตรวจสอบความพร้อมการใช้งานของระบบกล้อง และตรวจสอบการเก็บข้อมูลย้อนหลัง

10.8 กำหนดให้มีการทำแผนดำเนินการอัพเกรดระบบ Server อย่างสม่ำเสมอ

10.9 ในส่วนของห้อง server กำหนดให้ทีมไอทีบำรุงรักษาระบบห้อง server เป็นประจำทุกสัปดาห์ นอกจากนี้ในส่วนของคอมพิวเตอร์ส่วนบุคคลกำหนดให้ทีมไอทีแจ้งคำแนะนำขั้นพื้นฐานการดูแลคอมพิวเตอร์ให้แก่ผู้ใช้งาน

.....

(วีรทัศน์ จิรเดชวิโรจน์)

ผู้ช่วยกรรมการผู้จัดการใหญ่ – ฝ่ายการจัดการ

.....

(อัฐกร ทองถนอม)

ผู้อำนวยการฝ่ายกลยุทธ์และกระบวนการ