บริษัท ร้อกเวิร์ธ จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

---

1. วัตถุประสงค์

1.1 เพื่อใช้เป็นแนวทางสำหรับการปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึง และการใช้งานระบบสารสนเทศของบริษัทฯ

1.2 เพื่อให้ผู้รับผิดชอบ และผู้มีส่วนเกี่ยวข้อง ซึ่งได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ รับรู้ถึงแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ ตระหนักถึงความสำคัญ และให้ความร่วมมือปฏิบัติตามแนวทางที่กำหนดอย่างเคร่งครัด

2. ผู้รับผิดชอบ

กรรมการผู้อำนวยการใหญ่, ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และบุคลากรที่บริษัทฯแต่งตั้ง และมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ

3. นิยาม

3.1 ระบบสารสนเทศ หมายถึง ระบบสำหรับให้บริการ และจัดการข้อมูลสารสนเทศที่ใช้ในกิจการของบริษัทฯ ซึ่งได้แก่ ระบบอีอาร์พี (Infor LN), Intranet Website, ระบบจัดเก็บแบบ PDM, ระบบเงินเดือน, ระบบไฟล์กลางของบริษัทฯ, E-Mail, Internet Website, Active Directory, CCTV, Printer, Wi-Fi, Access Control

3.2 ระบบเครือข่ายสื่อสารข้อมูล หมายถึง การเชื่อมต่ออินเตอร์เน็ตผ่านสายสัญญาณ, การเชื่อมต่ออินเตอร์เน็ตผ่านเครือข่ายไร้สาย และการเชื่อมต่อเครือข่ายจากภายนอกผ่านอินเตอร์เน็ต (VPN)

3.3 เซิร์ฟเวอร์ หมายถึง เครื่องคอมพิวเตอร์ที่มีหน้าที่ให้บริการระบบสารสนเทศ

3.4 อุปกรณ์ระบบเครือข่าย หมายถึง อุปกรณ์ที่ทำหน้าที่ในการส่งผ่านข้อมูลระหว่างเครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ในระบบเครือข่ายสื่อสารข้อมูล ซึ่งอุปกรณ์ระบบเครือข่ายประกอบไปด้วย Router, Switching, Firewall, Wi-Fi Access Point, Wi-Fi Controller, Cables

3.5 เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์สำหรับผู้ใช้งานทั้งที่เป็นแบบ Desktop หรือ Laptop ซึ่งเครื่องคอมพิวเตอร์หนึ่งชุดจะประกอบไปด้วย CPU, Mainboard, Memory, Hard Disk, Power Supply, Monitor, Mouse, Keyboard

3.6 ระบบปฏิบัติการ หมายถึง ซอฟต์แวร์ซึ่งทำหน้าที่จัดการทรัพยากรต่างๆในเครื่องคอมพิวเตอร์ หรือเซิร์ฟเวอร์ และจัดการส่วนติดต่อกับผู้ใช้งาน อาทิเช่น Microsoft Windows, Linux, Mac OS เป็นต้น

3.7 โปรแกรมประยุกต์ หมายถึง ซอฟต์แวร์ที่นำมาติดตั้งบนเครื่องคอมพิวเตอร์ หรือซอฟต์แวร์ที่ทำงานผ่าน เว็บเบราว์เซอร์ เพื่อการใช้งานโดยผู้ใช้งาน อาทิเช่น Microsoft Office, Line เป็นต้น

3.8 ระบบจัดการฐานข้อมูล หมายถึง ซอฟต์แวร์ที่ทำหน้าที่ควบคุม และจัดการกับข้อมูลในฐานข้อมูล อาทิเช่น Microsoft SQL Server, MySQL เป็นต้น

3.9 อุปกรณ์ต่อพ่วง หมายถึง อุปกรณ์สำหรับใช้ในการนำข้อมูลเข้า และออกจากเครื่องเซิร์ฟเวอร์ หรือเครื่องคอมพิวเตอร์ เพื่อนำไปจัดเก็บ หรือจัดพิมพ์ อาทิเช่น เมาส์, คีย์บอร์ด, เครื่องสแกน, เครื่องพิมพ์, เครื่องสแกนลายนิ้วมือหรือหน้า, เครื่องสแกนบาร์โค้ด เป็นต้น

3.10 ผู้ดูแลระบบ หมายถึง ผู้ที่มีหน้าที่รับผิดชอบดูแลการทำงานของระบบสารสนเทศ การลงทะเบียนผู้ใช้งาน การสำรองข้อมูล การเรียกคืนข้อมูล การแก้ไขปัญหาในการใช้งานที่อาจเกิดขึ้น การเฝ้าระวังและตรวจสอบด้านความมั่นคงปลอดภัยของระบบและข้อมูล การประสานงานกับผู้พัฒนาระบบ เพื่อให้ระบบสารสนเทศสามารถใช้บริการได้อย่างเป็นปกติ และต่อเนื่อง

4. การควบคุมการเข้าถึง และการเข้าใช้งานระบบสารสนเทศ

4.1 ระบบงานสารสนเทศที่สำคัญของบริษัทฯ ซึ่งได้แก่

- ระบบ ERP (Infor LN)
- ระบบ Payroll (Business Plus)
- ระบบ Intranet (Intranetweb)
- ระบบ PDM (Engineering)
- ระบบ ไฟล์กลางของบริษัทฯ (Share Drive)
- ระบบ เชื่อมต่อทางไกล (Virtual Private Network – VPN)

ซึ่งมีความสำคัญต่อการดำเนินกิจการ และมีข้อมูลที่เป็นความลับของบริษัทฯ พนักงาน และลูกค้า ให้สร้างบัญชีผู้ใช้งาน (Username) แยกจากการเป็นรายบุคคล และกำหนดรหัสผ่าน (Password) สำหรับการเข้าใช้งานกับผู้ใช้งานแต่ละราย

4.2 กำหนดให้ผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายเป็นผู้รับผิดชอบ Password สำหรับบัญชีผู้ใช้งานสิทธิ์สูง ซึ่งได้แก่ บัญชี Root ของระบบปฏิบัติการ และระบบฐานข้อมูล และมีการควบคุมความปลอดภัยของการเข้าถึงและใช้รหัสผ่านดังนี้

4.2.1 มีการตั้งค่ารหัสผ่านในระดับระบบปฏิบัติการ (Operating System) ดังนี้

4.2.1.1 อายุรหัสผ่านใช้ได้ไม่เกิน 90 วัน

4.2.1.2 ความยาวของรหัสผ่านอย่างน้อย 8 ตัวอักษร

4.2.1.3 ความซับซ้อนของรหัสผ่าน กำหนดให้ต้องประกอบด้วย ตัวเลข ตัวอักษรภาษาอังกฤษ ทั้งที่เป็นตัวใหญ่และตัวเล็ก และอักขระพิเศษ (ได้แก่ # ! @ $ % & หรือ *) อย่างน้อย 1 ตัว

4.2.1.4 จำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 5 ครั้ง

4.2.1.5 จำนวนครั้งที่ไม่ให้กำหนดรหัสผ่านซ้ำกับรหัสผ่านเดิม 3 ครั้ง

ยกเว้นการตั้งค่ารหัสผ่านระดับ Database ทั้งในส่วนของฐานข้อมูล Microsoft SQL Server ของระบบต่างๆ เพื่อลดปัญหาจากการที่ Password หมดอายุ ซึ่งทำให้ Application ต่างๆที่เชื่อมต่อกับฐานข้อมูลไม่สามารถทำการเขียน หรืออ่านข้อมูลจากฐานข้อมูลได้ และจะต้องทำการดัดแปลงแก้ไข Application ด้วยทุกครั้งที่มีการเปลี่ยนแปลง Password ของระบบฐานข้อมูล (ทั้งนี้ได้ประเมินแล้วว่าจะไม่เป็นความ

เสี่ยงต่อความปลอดภัยของข้อมูล และฐานข้อมูล เนื่องจากผู้ใช้งานไม่สามารถเข้าถึงฐานข้อมูลได้โดยตรง)

4.2.2 การเข้าถึงระบบปฏิบัติการ และระบบฐานข้อมูล สามารถทำได้โดยผ่านระบบเครือข่ายส่วนบุคคลเสมือน (Virtual Private Network (VPN)) หรือระบบเครือข่ายภายใน (Local Area Network (LAN)) เท่านั้น โดยผู้ใช้งานจะต้อง Login ด้วย Username และ Password ของตนเองก่อนทุกครั้ง

4.3 การขออนุมัติ การอนุญาตให้เข้าใช้งาน การเปลี่ยนตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้าง และการระงับการเข้าใช้งานในระบบสารสนเทศที่มีความสำคัญ จะต้องมีบันทึกเก็บไว้เป็นหลักฐานเสมอ

4.4 การใช้งานระบบสารสนเทศอื่นๆ เช่น จดหมายอิเล็กทรอนิกส์ หรือเว็บไซต์ อนุญาตให้ใช้บัญชีรายชื่อแบบกลุ่มได้ตามความเหมาะสม และลักษณะการใช้งาน เช่น สาขา หน่วย หรือ ส่วนงานในสำนักงานใหญ่ เป็นต้น เพื่อไม่ให้เป็นอุปสรรคต่อการทำงาน

4.5 การกำหนดชื่อผู้ใช้งาน (Username) ให้กำหนดเป็นรหัสพนักงานโดยอ้างอิงจากระบบ HR System ที่ใช้งานเพื่อใช้ในการ Access เข้าระบบต่างๆของบริษัทฯ และตั้งชื่อภาษาอังกฤษด้วยตัวอักษรพิมพ์ใหญ่ หรือตัวอักษรพิมพ์เล็กให้ตรงกับชื่อในบัตรประชาชนของผู้ใช้งาน ส่วนการกำหนดชื่อผู้ใช้งาน จดหมายอิเล็กทรอนิกส์ ให้ใช้ชื่อภาษาอังกฤษด้วยตัวอักษรพิมพ์ใหญ่ หรือ ตัวอักษรพิมพ์เล็กให้ตรงกับชื่อในบัตรประชาชนของผู้ใช้งาน ตามด้วยจุด และตัวอักษรตัวแรกของนามสกุล หากซ้ำกับชื่อผู้ใช้งานที่มีอยู่แล้ว ให้ตามด้วยให้เพิ่มตัวอักษรตัวที่สองจากนามสกุล (หรือเพิ่มตัวอักษรในลำดับถัดไป) จนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น

5 หน้าที่ ความรับผิดชอบ และมารยาทในการใช้งานระบบสารสนเทศ (Users Duties, Responsibilities and Etiquette)

5.1 ผู้ใช้งานระบบมีหน้าที่เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับทันทีเมื่อเข้าใช้งานครั้งแรก ตั้งรหัสผ่านใหม่ที่คาดเดาได้ยาก รักษาความลับของรหัสผ่าน และเปลี่ยนรหัสผ่านทุก 90 วัน

5.2 ผู้ใช้งานมีหน้าที่เรียนรู้การใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงอย่างถูกวิธี และช่วยดูแลอุปกรณ์ที่ตนใช้งานเป็นประจำ หรือได้รับมอบหมายให้ดูแลให้ใช้งานได้เป็นปกติ เช่น ทำความสะอาด คอยสังเกตสัญญาณ หรือไฟเตือน และสังเกตการทำงานที่ผิดปกติของอุปกรณ์ และควรตรวจเช็คการทำงานของฮาร์ดดิสก์ และระบบไฟล์ข้อมูล (File System) โดยสม่ำเสมออย่างน้อยทุก 6 เดือน

5.3 ผู้ใช้งานต้องไม่ถอดถอน หยุดการทำงาน หรือดัดแปลงซอฟต์แวร์/โปรแกรมที่ติดตั้งไว้โดยผู้ดูแลระบบโดยเฉพาะโปรแกรมแอนติไวรัส แอนติมัลแวร์ เพราะเป็นสาเหตุและความเสี่ยงที่จะทำให้เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกติ หากไม่แน่ใจให้สอบถามกับผู้ดูแลระบบเสียก่อน

5.4 ผู้ใช้งานต้องไม่ดาวน์โหลดซอฟต์แวร์/โปรแกรมที่ไม่ได้รับการรับรอง ไม่มีลิขสิทธิ์ที่ถูกต้อง หรือมีความเสี่ยงต่อไวรัส และมัลแวร์ มาติดตั้งบนเครื่องคอมพิวเตอร์ที่ตนใช้งาน และควรใช้ความระมัดระวังในการเข้าเว็บไซต์บนอินเตอร์เน็ต ไม่คลิกปุ่มใดๆที่แสดงบนหน้าจอโดยการคาดเดา

5.5 ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ของบริษัทฯไปใช้ท่องเว็บไซต์ที่ไม่มีประโยชน์กับการทำงานเว็บไซต์ที่มีลักษณะต้องห้ามทางศีลธรรม ขัดต่อความสงบเรียบร้อย ขัดต่อกฎหมาย และเว็บไซต์ที่อาจมีความเสี่ยงต่อไวรัสและมัลแวร์ เช่น เล่นพนันออนไลน์ เล่นเกมส์ออนไลน์ ดูหนัง หรือภาพลามกอนาจาร การดาวน์โหลดไฟล์จากแหล่งที่ไม่รู้ที่มา เป็นต้น

5.6 ในเวลางาน ผู้ใช้งานต้องไม่ใช้อุปกรณ์ และเครือข่ายสื่อสารของบริษัทฯเข้าชม หรือดาวน์โหลดไฟล์มัลติมีเดียขนาดใหญ่ เช่น การดูคลิป ดูหนัง ฟังเพลง ดูการถ่ายทอดสดกีฬา ฯลฯ ซึ่งไม่เป็นประโยชน์กับการทำงาน เพราะเป็นการใช้ทรัพยากรเครือข่ายโดยไม่เหมาะสม และอาจส่งผลกระทบต่อการปฏิบัติงานของเพื่อนร่วมงาน

5.7 ผู้ใช้งานต้องไม่นำไฟล์ข้อมูลส่วนตัว เช่น เพลง รูปภาพ คลิป ซึ่งมีเนื้อหาที่ไม่เป็นประโยชน์ในการทำงานมาเก็บไว้ในเครื่องคอมพิวเตอร์ของบริษัทฯ

5.8 ผู้ใช้งานต้องไม่จัดเก็บ ไม่เปิดเสียงและภาพที่มีลักษณะขัดต่อศีลธรรม ผิดกฎหมาย สิ่งลามกอนาจาร และสื่อที่อาจทำให้เกิดความรู้สึกอึดอัดไม่สบายใจแก่เพื่อนร่วมงาน เช่น ความเห็นทางการเมือง และลัทธิความเชื่อทางศาสนา เป็นต้น

5.9 ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ เครื่องพิมพ์ เครื่องถ่ายเอกสาร และอุปกรณ์สารสนเทศที่เป็นทรัพย์สินของบริษัทฯ โดยเฉพาะสิ่งที่เป็นวัสดุสิ้นเปลือง ไปใช้ในเรื่องส่วนตัว และควรนำของส่วนตัวมาใช้เพื่อการดังกล่าว

5.10 ผู้ใช้งานต้องดูแลให้เครื่องคอมพิวเตอร์ได้รับการจ่ายไฟจากเครื่องสำรองไฟ UPS (ถ้ามี) และดูแลเครื่องสำรองไฟ UPS ยังสำรองไฟไว้ได้เมื่อไฟตก (แบตเตอรี่ของ UPS จะมีอายุการใช้งานโดยเฉลี่ย 1.5-2 ปี) เมื่อเครื่องสำรองไฟไม่ทำงานจะต้องรีบเปลี่ยนแบตเตอรี่ หรือเปลี่ยนเครื่องสำรองไฟโดยทันที เพราะเป็นความเสี่ยงที่จะทำให้ฮาร์ดดิสก์ และข้อมูลที่เก็บไว้เสียหายจนใช้การไม่ได้

5.11 หากเครื่องคอมพิวเตอร์ หรืออุปกรณ์พวงต่อที่ใช้งานมีปัญหา ให้ปรึกษากับผู้ดูแลระบบ เพื่อพิจารณาตัดสินใจในการแก้ไขปัญหา ไม่ควรนำไปซ่อมเองโดยพลการ เนื่องจากอาจทำให้เกิดเสียหายกับเครื่องคอมพิวเตอร์หรืออุปกรณ์พ่วงต่อ

6 หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (Duties and Responsibilities of System Administrators)

6.1 บริษัทฯมีหน้าที่จัดหาเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์พ่วงต่อที่มีคุณสมบัติเหมาะสมให้กับพนักงาน และมีหน้าที่ติดตั้งระบบปฏิบัติการ ซอฟต์แวร์ และโปรแกรมประยุกต์ให้พร้อมสำหรับการใช้งาน รวมถึงมีหน้าที่ซ่อมแซม จัดหาอะไหล่ ให้คำปรึกษาในการใช้งานและการซ่อมบำรุงแก่ผู้ใช้งาน

6.2 ให้ผู้ดูแลระบบมีหน้าที่ควบคุมสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของผู้ใช้งาน สิทธิ์ในการเข้าใช้งาน ได้แก่ ให้อ่านอย่างเดียว, ให้สร้างข้อมูลได้, ให้แก้ไขข้อมูลได้, ให้อนุมัติได้, ไม่มีสิทธิ์ใช้งาน ตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

6.3 ผู้ใช้งานที่จะเข้าใช้งานระบบสารสนเทศได้ จะต้องเป็นไปตามนโยบายที่บริษัทฯกำหนด หรือได้อนุญาตจากกรรมการผู้อำนวยการใหญ่ หรือรองกรรมการผู้อำนวยการใหญ่ หรือผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และให้มีการทบทวนสิทธิผู้ใช้งานในระบบ อย่างน้อยปีละ 1 ครั้ง

6.4 ระบบสารสนเทศทุกระบบจะต้องมีการกำหนด และมอบหมายหน้าที่ในการดูแลระบบ (System Administration) ให้กับผู้ดูแลระบบ (System Administrator) และจัดทำกรอบหน้าที่ไว้อย่างชัดเจน

6.5 หน้าที่ของผู้ดูแลระบบ (System Administrator) ต้องประกอบด้วยเรื่องต่อไปนี้เป็นอย่างน้อย

6.5.1 จัดทำบัญชีรายชื่อผู้ใช้งาน

6.5.2 ตั้ง หรือเปลี่ยนรหัสผ่าน

6.5.3 รักษาความปลอดภัยในการเข้าถึง และใช้งานระบบให้เป็นไปตามนโยบายของบริษัทฯ

6.5.4 ทำการสำรองข้อมูล และทดสอบการเรียกคืนข้อมูลในระบบตามระยะเวลาที่กำหนด

6.5.5 ตรวจสอบสภาวะการทำงานของระบบอย่างสม่ำเสมอ

6.5.6 รับผิดชอบในการแก้ไขปัญหาเพื่อให้ระบบสารสนเทศทำงานได้เป็นปกติ

6.5.7 ให้คำปรึกษาแก่ผู้ใช้งาน

7 การใช้งานระบบเครือข่ายสื่อสาร

7.1 ให้อุปกรณ์เครือข่าย เซิร์ฟเวอร์ เครื่องพิมพ์ และอุปกรณ์ส่วนกลางทุกชิ้นที่อยู่บนเครือข่ายสื่อสารของบริษัทฯ มีการกำหนดหมายเลขไอพีแอดเดรส (IP Address) แบบค่าคงที่ (Static) และให้ทำทะเบียนหมายเลขไอพีไว้ด้วย

7.2 ให้อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ทุกเครื่อง ที่อยู่บนเครือข่ายสื่อสารของบริษัทฯมีการกำหนดหมายเลขไอพีแอดเดรส (IP Address) แบบไดนามิก (Dhcp)

7.3 ให้เปิดไฟร์วอลล์ (Firewall) และควบคุมการเปิดพอร์ต (Port) ในการใช้งานเท่าที่จำเป็นเท่านั้น และให้ทำทะเบียนพอร์ตที่เปิดใช้งานไว้ด้วย

7.4 ห้ามมิให้พนักงานนำอุปกรณ์เครือข่ายมาติดตั้งเองโดยพลการ การติดตั้งอุปกรณ์เครือข่าย เช่น เราเตอร์ (Router) ไวไฟเราเตอร์ (Wi-fi Router) แอคเซสพอยต์ (Access Point) สวิตช์ (Switch) ในบริษัทฯ จะต้องได้รับการอนุญาตจากผู้ดูแลระบบเสียก่อน ทั้งนี้เพื่อป้องกันความเสียหายต่อการทำงานของระบบเครือข่าย

8 การรักษาความลับของข้อมูล (Secrecy of Data)

8.1 ห้ามมิให้พนักงานเปิดเผย เผยแพร่ แก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้อง หรือทำสำเนา โยกย้ายออกสู่ภายนอก ซึ่งข้อมูลที่เป็นความลับที่อยู่ในระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด

8.2 ข้อมูลที่เป็นความลับประกอบด้วย

8.2.1 ข้อมูล และรายงานทางบัญชี

8.2.2 ข้อมูล และรายงานทางการเงิน

8.2.3 งบประมาณ

8.2.4 ข้อมูลประวัติ และรายได้ของพนักงาน

8.2.5 นโยบาย หรือคำสั่งที่ยังไม่ได้รับอนุญาตให้ทำการเผยแพร่

8.2.6 ยุทธศาสตร์ และแผนธุรกิจ

8.2.7 ข้อมูลส่วนบุคคล และประวัติการทำสินเชื่อของลูกค้า

ข้อมูลที่เชื่อมโยงกับรายการดังกล่าวข้างต้น เช่น ข้อมูลเชิงวิเคราะห์ต่างๆ เป็นต้น

8.3 การแลกเปลี่ยนข้อมูลที่เป็นความลับ ให้ผู้จัดทำ และเจ้าของข้อมูลจัดเก็บไว้ในพื้นที่ส่วนตัวเท่านั้น หากมีความจำเป็นจะต้องแลกเปลี่ยนข้อมูลที่เป็นความลับด้วยวิธีการอิเล็กทรอนิกส์ ให้เจ้าของข้อมูลทำการเข้ารหัสไฟล์ข้อมูลเพื่อป้องกันการเปิดอ่านโดยบุคคลอื่น แจ้งรหัสสำหรับเปิดอ่านไฟล์ให้กับผู้รับข้อมูล และลบไฟล์ออกจากพื้นที่แลกเปลี่ยนข้อมูลเมื่อผู้รับได้รับข้อมูลแล้ว

9 ห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) และการติดตั้งอุปกรณ์ (Equipment Installation)

9.1 เครื่องเซิร์ฟเวอร์ (Server) และอุปกรณ์เครือข่าย (Network Equipment) ที่เป็นส่วนประกอบของระบบสารสนเทศของบริษัทฯ ให้ติดตั้งในห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) หรือในสถานที่เฉพาะที่กำหนดไว้ และอนุญาตให้เข้าถึงได้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น

9.2 การเข้าไปปฏิบัติงานในห้องอุปกรณ์เซิร์ฟเวอร์ จะต้องมีการบันทึกไว้ในสมุดบันทึกทุกครั้ง พร้อมรายละเอียดได้แก่ ชื่อ เวลาเข้า-ออก เรื่องที่เข้าไปดำเนินการ และลายมือชื่อ หากเป็นบุคคลภายนอกจะต้องมีลายมือชื่อของผู้กำกับงานของบริษัทฯร่วมอยู่ด้วยทุกครั้ง

9.3 ห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) ต้องมีการควบคุมอุณหภูมิ ความชื้น และฝุ่นละอองไว้อย่างเหมาะสมตลอดเวลา และควรจัดให้มีระบบแจ้งเตือน เมื่อมีความผิดปกติเกิดขึ้น

9.4 เครื่องเซิร์ฟเวอร์ และอุปกรณ์เครือข่าย ให้ติดตั้งและจัดวางในตู้อุปกรณ์ (Rack) การเดินสายสัญญาณให้จัดวางด้วยความเป็นระเบียบเรียบร้อย และให้จัดทำป้ายชื่อ (Label) และแผนผัง (Diagram) การเดินสายสัญญาณและผังการเชื่อมต่ออุปกรณ์เครือข่าย

9.5 ให้ทำป้ายชื่อกำกับติดไว้บนเครื่องเซิร์ฟเวอร์ อุปกรณ์เครือข่าย สายสัญญาณ ร่วมกับการพิจารณาใช้สายสัญญาณที่มีสีแตกต่างกัน เพื่อป้องกันการเชื่อมต่อสายสัญญาณผิดเส้น

10 การป้องกันการหยุดชะงักของระบบ (Fault Tolerance)

10.1 เครื่องเซิร์ฟเวอร์ของระบบสารสนเทศจะต้องติดตั้งฮาร์ดดิสก์จำนวนอย่างน้อย 2 ลูก และตั้งให้มีการทำงานซ้ำซ้อนกัน (Redundancy) อย่างน้อยในแบบ RAID 1,5,6,10 หรือในแบบอื่นที่เทียบเท่ากันหรือดีกว่า เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลในกรณีที่ฮาร์ดดิสก์ลูกใดลูกหนึ่งเสียอย่างกะทันหัน

10.2 เครื่องเซิร์ฟเวอร์ของระบบสารสนเทศควรมีอย่างน้อย 2 ชุด ให้ทำงานควบคู่กันในลักษณะ Active/Active หรือ Active/Standby หรือจัดให้มีเครื่องเซิร์ฟเวอร์สำรองไว้เพื่อให้สามารถนำมาใช้งานแทนกันได้ภายในเวลา 2 ชั่วโมง

10.3 เครื่องเซิร์ฟเวอร์ของระบบสารสนเทศ ควรจะต้องติดตั้งส่วนจ่ายไฟ (PSU) จำนวน 2 ชุด ที่ได้รับการจ่ายไฟจากเครื่องสำรองไฟ (UPS) จำนวน 2 ชุด ที่แยกจากกัน

10.4 เครื่องเซิร์ฟเวอร์ และอุปกรณ์เครือข่ายจะต้องได้รับการจ่ายไฟจากเครื่องสำรองไฟ (UPS) เท่านั้น เพื่อป้องกันไม่ให้การทำงานหยุดชะงัก เมื่อไฟตกหรือไฟดับ และป้องกันความเสียหายที่อาจเกิดขึ้นได้กับฮาร์ดดิสก์ (Hard Disk) และระบบไฟล์ข้อมูล (File System) จากเหตุดังกล่าว

10.5 เครื่องสำรองไฟของระบบสารสนเทศควรสำรองไฟได้ไม่น้อยกว่า 30 นาที เพื่อให้ผู้ดูแลระบบมีเวลามากพอในการดำเนินการปิดระบบ (Shutdown) อย่างเป็นขั้นตอน เพื่อป้องกันข้อมูลสูญหาย และความเสียหายที่อาจจะเกิดขึ้นกับฮาร์ดดิสก์ (Hard Disk) หรือระบบไฟล์ (File System) หรือระบบฐานข้อมูล (Database)

10.6 ตั้งค่าให้เครื่องเซิร์ฟเวอร์ปิดตัวเอง (Shutdown) ได้โดยอัตโนมัติ เมื่อพบว่ามีการจ่ายไฟจากแบตเตอรี่ของเครื่องสำรองไฟนานเกินกว่า 30 นาที

10.7 จัดให้มีช่องทางสำรองในการเชื่อมต่อกับอินเตอร์เน็ตในกรณีที่ช่องทางหลักไม่สามารถใช้การได้

11 การสำรองข้อมูล และการเรียกคืน (Backup and Recovery)

11.1 ระบบสารสนเทศที่มีการเพิ่ม เปลี่ยนแปลง หรือแก้ไขข้อมูลเป็นประจำทุกวัน ให้มีการสำรองข้อมูลในระบบทุกวัน

11.2 ระบบสารสนเทศที่มีการเพิ่ม เปลี่ยนแปลง หรือแก้ไขข้อมูลเป็นประจำทุกสัปดาห์ หรือทุกเดือน ให้มีการสำรองข้อมูลในระบบตามรอบระยะเวลาดังกล่าว

11.3 ข้อมูลจากระบบสารสนเทศที่จะต้องมีการทำสำรองได้แก่ ข้อมูลของผู้ใช้งาน (User Data), ข้อมูลการติดตั้งและปรับแต่งระบบ (Configuration Files) และข้อมูลอื่นๆที่เกี่ยวกับผู้ใช้งาน โดยข้อมูลที่สำรองไว้ให้แยกเก็บไว้ต่างหากจากเครื่องเซิร์ฟเวอร์ที่กำลังใช้งาน

11.4 ในกรณีที่ระบบสารสนเทศระบบใดระบบหนึ่งเกิดการล้มเหลวโดยกะทันหัน จะต้องมีระบบสำรอง หรือวิธีการที่ทำให้สามารถเรียกคืนการทำงานได้ภายในระยะเวลา 2 ชั่วโมง

11.5 ให้มีการทบทวน และทดสอบการสำรองข้อมูล และการเรียกคืนข้อมูลจากระบบสารสนเทศที่ใช้ปฏิบัติการให้เป็นไปตามนโยบายข้างต้น อย่างน้อยปีละ 1 ครั้ง และระบบงานที่จ้างบุคคลภายนอกดูแล ฐานข้อมูลสำรอง

12 การเก็บบันทึกประวัติการเข้าใช้งาน (Logging)

12.1 ให้มีการจัดเก็บบันทึกประวัติการเข้าใช้งาน (Login) ประวัติการใช้งาน (Usage) ในระบบที่สำคัญ และให้เป็นไปตามข้อกำหนดของกฎหมาย

13 ระบบการแจ้งเตือนสถานะของการทำงาน (Monitoring)

13.1 จะต้องจัดให้มีการแจ้งเตือนสถานะของทำงาน (Monitoring) ของระบบเครือข่าย และเครื่องเซิร์ฟเวอร์ของระบบสารสนเทศ โดยผู้ดูแลระบบสามารถตรวจสอบสถานะการทำงาน และการแจ้งเตือนได้จากระยะไกล

14 คู่มือการใช้งาน และดูแลระบบสารสนเทศ (Documentation)

14.1 ให้จัดทำคู่มือการใช้งาน การติดตั้ง การดูแลรักษา การสำรองและการเรียกคืนข้อมูล ของระบบสารสนเทศ โดยให้มีรายละเอียดที่จำเป็นสำหรับการดูแลรักษาระบบอย่างครบถ้วน เพียงพอ และอ่านเข้าใจได้อย่างชัดเจน

14.2 ให้มีการจัดทำทะเบียนระบบสารสนเทศ ประกอบไปด้วยข้อมูลที่สำคัญของแต่ละระบบ ได้แก่ ชื่อระบบ บริการของระบบโดยสังเขป กลุ่มผู้ใช้งาน คุณลักษณะของเซิร์ฟเวอร์ (ยี่ห้อและรุ่น ซีพียู จำนวนหน่วยความจำ ฮาร์ดดิสก์และความจุ) ระบบปฏิบัติการที่ติดตั้ง ซอฟต์แวร์ที่ติดตั้ง การตั้งค่าต่างๆของระบบ (Configuration) ไอพีแอดเดรส (IP Address) แผนภาพแสดงลักษณะโครงสร้าง ชื่อบัญชีผู้ดูแลระบบ (รหัสผ่านให้แจ้งต่างหาก) ชื่อและข้อมูลติดต่อของผู้ดูแลระบบ ผู้จัดทำทะเบียน วันที่ที่จัดทำทะเบียน เป็นต้น

14.3 ทะเบียนระบบสารสนเทศจะต้องได้รับการทบทวนปรับปรุงตามระยะเวลาที่กำหนด อย่างน้อยปีละ 1 ครั้ง

14.4 ให้รวบรวมและจัดเก็บข้อมูลคุณลักษณะของอุปกรณ์ (Specification) และคู่มือการใช้งาน (Manual) ของทั้งฮาร์ดแวร์ และซอฟต์แวร์ของระบบสารสนเทศ ในรูปแบบของไฟล์อิเล็กทรอนิกส์ เก็บไว้อย่างน้อย 1 ชุด

15 การบำรุงรักษา และการสำรองอะไหล่ (Spare Parts)

15.1 ให้ประเมินความเหมาะสมของเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์ต่อพ่วงต่อระบบปฏิบัติการ ซอฟต์แวร์ และโปรแกรมประยุกต์ ที่มีการใช้งานในบริษัทฯ ตามประสิทธิภาพการทำงาน อายุการใช้งาน ความเหมาะสมในการใช้งาน ค่าใช้จ่ายในการซ่อมบำรุง และการสำรองอะไหล่ เพื่อจัดตั้งงบประมาณในการจัดซื้อ จัดหาอุปกรณ์ใหม่มาใช้งานทดแทน อย่างน้อยปีละ 1 ครั้ง

16 ขั้นตอนปฏิบัติการจัดการบัญชีผู้ใช้งานในระบบ

16.1 ข้อปฏิบัติในการเพิ่ม/เปลี่ยนแปลง/ระงับ สิทธิการใช้งานในระบบ

16.1.1 การเพิ่มสิทธิให้กับพนักงานใหม่

16.1.1.1 ฝ่ายเทคโนโลยีสารสนเทศ รับคำสั่งการเพิ่มพนักงานทดลองงานจากฝ่ายทรัพยากรมนุษย์ฯ ที่ได้รับอนุมัติจากกรรมการผู้อำนวยการใหญ่

16.1.1.2 ฝ่ายเทคโนโลยีสารสนเทศ เพิ่มข้อมูล ชื่อ-สกุล ตำแหน่ง และสังกัดสาขา หน่วย ในระบบให้ถูกต้องเป็นไปตามตำแหน่งงาน

16.1.1.3 ฝ่ายเทคโนโลยีสารสนเทศ เพิ่มชื่อผู้ใช้งาน และรหัสผ่าน รวมถึงสิทธิ การใช้งาน และการเข้าถึงข้อมูลให้เป็นไปตามตำแหน่งงาน

16.1.1.4 ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศตรวจสอบการเพิ่มข้อมูลพนักงาน และสิทธิการใช้งาน และการเข้าถึงข้อมูลในระบบ

16.1.1.5 ฝ่ายเทคโนโลยีสารสนเทศแจ้งข้อมูล ชื่อผู้ใช้งาน และรหัสผ่าน ให้พนักงานทดลองทราบในวันแรกของการทำงาน

16.1.2 การเปลี่ยนแปลงสิทธิในระบบ กรณีที่มีการโยกย้าย หรือเปลี่ยนตำแหน่งงาน

16.1.2.1 ฝ่ายเทคโนโลยีสารสนเทศ รับคำสั่งการเปลี่ยนแปลงตำแหน่ง หรือโยกย้าย สถานที่ทำงานจากฝ่ายบุคคลที่ได้รับการอนุมัติจากกรรมการผู้อำนวยการใหญ่

16.1.2.2 ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการ เปลี่ยนแปลงหรือโยกย้าย พนักงานในระบบตามคำสั่งที่ได้รับการอนุมัติ

16.1.2.3 ฝ่ายเทคโนโลยีสารสนเทศ ปรับปรุงสิทธิการเข้าใช้งานในระบบตามตำแหน่งงาน

16.1.2.4 หัวหน้าแผนกเทคโนโลยีสารสนเทศ ตรวจสอบการเปลี่ยนแปลง โยกย้าย และการกำหนดสิทธิในระบบ

16.1.3 การระงับ หรือ Disable บัญชีรายชื่อผู้ใช้งานในระบบ กรณีพนักงานลาออก หรือมีคำสั่งให้พักงาน และออกจากการเป็นพนักงาน

16.1.3.1 ฝ่ายเทคโนโลยีสารสนเทศ รับคำสั่งพนักงานลาออก พักงาน หรือให้ออก จากฝ่ายทรัพยากรมนุษย์ฯ ที่อนุมัติจากกรรมการผู้อำนายการใหญ่

16.1.3.2 ฝ่ายเทคโนโลยีสารสนเทศ ระงับสิทธิการใช้งานในระบบของพนักงานคนดังกล่าว

16.1.3.3 หัวหน้าแผนกเทคโนโลยีสารสนเทศ ตรวจสอบการระงับสิทธิในระบบ

16.1.4 กรณีมีการขอเปลี่ยนแปลง เพิ่ม/ลบ สิทธิการใช้งานในบางเมนูงาน

16.1.4.1 หัวหน้าในส่วนงานที่ต้องการปรับเปลี่ยนสิทธิการเข้าใช้งานระบบ จะต้องทำการแจ้งผ่านระบบ Service Request เพื่อขอเปลี่ยนแปลงสิทธิการใช้งานของพนักงานในสังกัด

16.1.4.2 ฝ่ายเทคโนโลยีสารสนเทศดำเนินการเปลี่ยนแปลงสิทธิในระบบงาน

16.1.4.3 ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศตรวจสอบการเปลี่ยนสิทธิในระบบงาน

16.1.4.4 ฝ่ายเทคโนโลยีสารสนเทศแจ้งผลการดำเนินการเปลี่ยนแปลงให้ผู้ร้องขอทราบเพื่อเข้าใช้งานในระบบ

17 ขั้นตอนปฏิบัติในการเปลี่ยนแปลง แก้ไข และการพัฒนาระบบสารสนเทศ

17.1 ขั้นตอนการพัฒนาระบบงานสารสนเทศตามแผนงาน และโครงการประจำปี

17.1.1 ฝ่ายเทคโนโลยีสารสนเทศจัดทำแผนโครงการ และรายละเอียดการพัฒนาเสนอต่อ กรรมการผู้อำนวยการใหญ่พิจารณาอนุมัติโครงการ

17.1.2 จัดทำรายละเอียดขออนุมัติแก้ไข/ปรับปรุงระบบ ตามแผนงานโครงการที่ได้รับอนุมัติ

17.1.3 ดำเนินการส่งเอกสารรายละเอียดให้ผู้พัฒนาระบบ แก้ไข/ปรับปรุงระบบ

17.1.4 ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบทดสอบ (Development System)

17.1.5 ฝ่ายเทคโนโลยีสารสนเทศ และผู้ใช้งานตรวจสอบข้อมูลในระบบทดสอบ

17.1.6 ฝ่ายเทคโนโลยีสารสนเทศ ยืนยันความถูกต้อง และแจ้งให้ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบ (Production System)

17.1.7 ฝ่ายเทคโนโลยีสารสนเทศ ติดตามประเมินผลการแก้ไขเปลี่ยนแปลงหลังจากมีการปรับปรุง

17.2 ขั้นตอนการแก้ไขเปลี่ยนแปลงระบบตามนโยบาย หรือตามมติที่ประชุมของฝ่ายต่างๆ

17.2.1 ฝ่ายเทคโนโลยีสารสนเทศ ได้รับแจ้งให้มีการปรับปรุงเปลี่ยนแปลง หรือพัฒนาระบบจากมติที่ประชุมของส่วนงานต่างๆ

17.2.2 ฝ่ายเทคโนโลยีสารสนเทศ หรือส่วนงานที่เกี่ยวข้อง เสนอขออนุมัติการแก้ไขโปรแกรม จากกรรมการผู้อำนวยการใหญ่

17.2.3 ฝ่ายเทคโนโลยีสารสนเทศ ดำเนินการแจ้งผู้พัฒนาระบบแก้ไขโปรแกรม

17.2.4 ผู้พัฒนาระบบนำโปรแกรมขึ้นทดสอบระบบ (Development System)

17.2.5 ฝ่ายเทคโนโลยีสารสนเทศ และผู้ใช้งานตรวจสอบข้อมูลในระบบทดสอบ

17.2.6 ฝ่ายเทคโนโลยีสารสนเทศ ยืนยันความถูกต้องของโปรแกรม และแจ้งให้ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบ (Production System)

17.2.7 ฝ่ายเทคโนโลยีสารสนเทศ ติดตามประเมินผลการแก้ไขเปลี่ยนแปลงหลังจากมีการปรับปรุง

ทั้งนี้ โดยนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้รับอนุมัติจากคณะกรรมการบริหาร ในที่ประชุม เมื่อวันที่ 19 มีนาคม 2567

(นายดุษฎี พงษ์สุทธิมนัส)

กรรมการผู้อำนวยการใหญ่