710/2568

บริษัท ศักดิ์สยามลิสซิ่ง จำกัด (มหาชน) 25 พฤศจิกายน 2568

เรื่อง นโยบายการใช้งานระบบสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล

เพื่อให้นโยบายการใช้งานระบบสารสนเทศและระบบเครือข่ายสื่อสารข้อมูลของบริษัทฯ มีรายละเอียดที่ครบถ้วนและเหมาะสมกับการทำงานมากยิ่งขึ้น จึงขอยกเลิก ประกาศ เรื่อง นโยบายการใช้งานระบบสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล เลขที่ 884/2567 ลงวันที่ 27 ธันวาคม 2567 และใช้ประกาศฉบับนี้แทน

1. วัตถุประสงค์

1.1 เพื่อใช้เป็นแนวทางสำหรับการปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัย (Security) ที่เกี่ยวข้องกับการควบคุมการเข้าถึง (Access) และการใช้งานระบบสารสนเทศของบริษัทฯ

1.2 เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ซึ่งได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท รับรู้ถึงแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ ตระหนักถึงความสำคัญ และให้ความร่วมมือปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด

2. ผู้รับผิดชอบ

กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้จัดการฝ่ายสารสนเทศ และบุคลากรที่บริษัทแต่งตั้งและมอบหมายให้ดูแลระบบสารสนเทศของบริษัทฯ

3. คำนิยาม

คำนิยามในหัวข้อต่าง ๆ ต่อไปนี้ เป็นคำนิยามที่ทางบริษัทฯ ได้กล่าวไว้เพื่อเป็นการสื่อสารให้เกิดความเข้าใจตรงกันในเอกสารนโยบายฉบับนี้ ซึ่งมีรายละเอียดดังต่อไปนี้

3.1 ระบบสารสนเทศ (Information Systems) หมายถึง องค์ประกอบต่าง ๆ ที่มีความเกี่ยวข้องและทำงานประสานกันในการเก็บรวบรวม บันทึก ประมวลผล จัดเก็บและแจกจ่ายสารสนเทศ เพื่อสนับสนุนการตัดสินใจและหน้าที่ทางการบริหาร ได้แก่ การวางแผน การจัดองค์กร การประสานงาน การควบคุมและการสื่อสารภายในองค์กร และเป็นระบบงานสารสนเทศที่เกี่ยวข้องกับการให้บริการลูกค้า ระบบงานด้านการบริหารงานต่าง ๆ และระบบการจัดการข้อมูลสารสนเทศที่ใช้ในกิจการของบริษัทฯ (รายละเอียดตามเอกสารแนบ)

3.2 ระบบเครือข่ายสื่อสารข้อมูล (Data Communication Network) หมายถึง ระบบเครือข่ายที่ทำหน้าที่ในการเชื่อมต่อข้อมูลระหว่างสำนักงานใหญ่ สาขา หน่วยของบริษัทฯ ซึ่งครอบคลุมการเชื่อมต่อผ่านระบบเครือข่ายอินเตอร์เน็ต (Internet), อินทราเน็ต (Intranet) และระบบเครือข่ายไร้สาย (Wireless LAN) ของบริษัทฯ

3.3 เซิร์ฟเวอร์ (Server) หมายถึง เครื่องคอมพิวเตอร์ที่มีหน้าที่ให้บริการระบบสารสนเทศของบริษัทฯ ได้แก่ Web Server, Database Server, Mail Server, File Server, Application Server, Virtual Server และ Hyper Converged Infrastructure (HCI) เป็นต้น

3.4 อุปกรณ์ระบบเครือข่าย (Network Equipment) หมายถึง อุปกรณ์ที่ทำหน้าที่ในการส่งผ่านข้อมูลระหว่างเครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ อุปกรณ์พ่วงต่อ ในระบบเครือข่ายสื่อสารข้อมูล ซึ่งอุปกรณ์ระบบเครือข่ายประกอบไปด้วย เราเตอร์ (Router), สวิตช์ (Network Switch), โหลดบาลานเซอร์ (Load Balancer), ไฟร์วอลล์ (Firewall), แอคเซสพอยท์ (Wi-fi Access Point), เครื่องควบคุมการทำงานไวไฟ (Wi-fi Controller) และสายสัญญาณ (Cables)

3.5 เครื่องคอมพิวเตอร์ หมายถึง คอมพิวเตอร์สำหรับผู้ใช้งานในแบบต่าง ๆ จะประกอบไปด้วย ซีพียู (CPU), เมนบอร์ด (Mainboard), หน่วยความจำ (Memory), ฮาร์ดดิสก์ (Hard Disk), ส่วนจ่ายไฟ (Power Supply Unit: PSU), มอนิเตอร์ (Monitor), เมาส์ (Mouse), คีย์บอร์ด (Keyboard) และให้รวมเครื่องสำรองไฟ (Uninterruptible Power Supply: UPS) หรือแบตเตอรี่สำรองไฟ (Battery) เข้าไว้ด้วย และรวมถึงยังอุปกรณ์ส่วนอื่น ๆ ดังนี้

3.5.1 เดสก์ท็อป (Desktop) คอมพิวเตอร์ที่ถูกออกแบบมาให้ใช้งานในที่ตั้งถาวรบนโต๊ะไม่เน้นการปรับเปลี่ยนหรือให้ง่ายต่อการเคลื่อนที่

3.5.2 แล็ปท็อป (Laptop) คอมพิวเตอร์พกพาที่รวมหน้าจอ แป้นพิมพ์ และหน่วยประมวลผลไว้ในตัว ออกแบบมาให้มีขนาดเล็ก

3.5.3 แท็บเล็ต (Tablet) คอมพิวเตอร์พกพาที่มีหน้าจอสัมผัส ใช้แทนเมาส์และคีย์บอร์ด มีหน่วยประมวลผล, หน่วยความจำ, และแบตเตอรี่ในตัว

3.6 ระบบปฏิบัติการ (Operating System) หมายถึง ซอฟท์แวร์ซึ่งทำหน้าที่จัดการทรัพยากรต่าง ๆ ในเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ และจัดการส่วนติดต่อกับผู้ใช้งาน ตัวอย่างของระบบปฏิบัติการได้แก่ Microsoft Windows, Linux, FreeBSD, Android และ IOS เป็นต้น

3.7 โปรแกรมประยุกต์ (Application Software) หมายถึง โปรแกรมที่นำมาติดตั้งบนเครื่องคอมพิวเตอร์หรือโปรแกรมที่ทำงานผ่านทางเว็บเบราว์เซอร์ ซึ่งเป็นโปรแกรมสำเร็จรูปหรือโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อใช้ประโยชน์ในการทำงาน ตัวอย่างของโปรแกรมประยุกต์ได้แก่ โปรแกรม Microsoft Office, Google Workspace, Google Drive, LINE เป็นต้น

3.8 ระบบจัดการฐานข้อมูล (Database Management System) หมายถึง ซอฟท์แวร์ที่ทำหน้าที่ควบคุมและจัดการกับข้อมูลในฐานข้อมูล (Database) ตัวอย่างของระบบจัดการฐานข้อมูลมีดังนี้

- NoSQL Databases ได้แก่ Mongo DB
- Relational Database ได้แก่ MySQL, MariaDB, MSSQL, Oracle Database, Sybase

3.9 อุปกรณ์พ่วงต่อ (Peripherals) หมายถึง อุปกรณ์สำหรับใช้ในการนำข้อมูลเข้าและออกจากเครื่องเซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์ เพื่อนำไปจัดเก็บหรือจัดพิมพ์ ตัวอย่างเช่น เมาส์, คีย์บอร์ด, เครื่องสแกนภาพ, เครื่องพิมพ์เลเซอร์, เครื่องพิมพ์อิงค์เจ็ท, เครื่องพิมพ์หัวเข็ม, เครื่องสแกนลายนิ้วมือ, เครื่องสแกนบาร์โค้ด, USB Drive, เครื่องอ่านบัตรประชาชน (Smart Card Reader) เป็นต้น

3.10 ผู้ดูแลระบบ (System Administrator หรือ Sysadmin) หมายถึง ผู้มีหน้าที่รับผิดชอบดูแลการทำงานของระบบสารสนเทศ การลงทะเบียนผู้ใช้งาน การสำรองข้อมูล การเรียกคืนข้อมูล การแก้ไขปัญหาในการใช้งานที่อาจเกิดขึ้น การเฝ้าระวังและตรวจสอบด้านความมั่นคงปลอดภัยของระบบและข้อมูล การประสานงานกับผู้พัฒนาระบบ เพื่อให้ระบบสารสนเทศสามารถให้บริการกับผู้ใช้งานได้อย่างมีประสิทธิภาพ

4. การควบคุมการเข้าถึงและการเข้าใช้งานระบบสารสนเทศ (Access Control)

การควบคุมการเข้าถึง และการกำหนดสิทธิในการใช้งานระบบสารสนเทศ รวมถึงแก้ไขระบบงานต่าง ๆ ของบริษัทฯ ต้องเป็นไปตามนโยบาย ซึ่งระบบและข้อมูลต่าง ๆ เป็นทรัพย์สินของทางบริษัทฯ หากจะดำเนินการแก้ไข ปรับปรุง เข้าถึงจะต้องได้รับมอบหมายจากผู้จัดการฝ่ายสารสนเทศ จึงได้กำหนดนโยบายเพื่อเป็นแนวทางในการปฏิบัติและควบคุมการทำงานดังนี้

4.1 ระบบงานสารสนเทศที่เกี่ยวข้องกับการให้บริการลูกค้า ซึ่งได้แก่ ระบบงานสินเชื่อ LMIS, ระบบงานสินเชื่อเช่าซื้อ (HPS) และระบบงานจ่ายสินเชื่อให้ลูกค้า (SAK Payment) ซึ่งเป็นระบบที่มีความสำคัญต่อการดำเนินกิจการของบริษัทฯ รวมถึงมีข้อมูลที่เป็นความลับของบริษัทฯ และข้อมูลของลูกค้า ซึ่งทางบริษัทฯ จะต้องเก็บข้อมูลเป็นความลับ โดยบริษัทฯ กำหนดนโยบายให้มีการเข้าใช้งานระบบผ่าน Username และ Password ตามสิทธิของผู้ใช้งานแต่ละระบบ

4.2 ระบบงานด้านการบริหารของบริษัทฯ ซึ่งได้แก่ ระบบงานบัญชีเงินเดือน ข้อมูลพนักงาน ระบบงานบัญชี SAP และระบบไฟล์กลางสำนักงานใหญ่ โดยบริษัทฯ กำหนดนโยบายให้มีการเข้าใช้งานระบบผ่าน Username และ Password สำหรับผู้ใช้งานที่เกี่ยวข้องเท่านั้น

4.3 ระบบงานการแก้ไขข้อมูล (DMT) เป็นระบบงานที่ใช้สำหรับการเข้าถึงข้อมูล ซึ่งผู้ใช้งานระบบนี้จะต้องเป็นผู้มีสิทธิในการเข้าถึงข้อมูล เพื่อทำการแก้ไข เพิ่ม หรือ ลบข้อมูลต่าง ๆ ได้

4.4 ระบบงานสารสนเทศอื่น ๆ เช่น จดหมายอิเล็กทรอนิกส์ หรือเว็บไซต์ อนุญาตให้ใช้บัญชีรายชื่อแบบกลุ่มได้ตามความเหมาะสมและลักษณะการใช้งาน เช่น สาขา หน่วย หรือส่วนงานในสำนักงานใหญ่ เป็นต้น เพื่อไม่ให้เป็นอุปสรรคต่อการทำงาน

5. การกำหนดสิทธิในการเข้าใช้งานระบบสารสนเทศ

การกำหนดสิทธิในการเข้าถึงและการใช้งานของระบบสารสนเทศของบริษัทฯ อยู่ในความรับผิดชอบของผู้ที่ได้รับมอบหมาย โดยแบ่งตามระดับของการใช้งานดังนี้

5.1 การกำหนดรหัสผ่านระดับผู้ปฏิบัติการ หรือ ผู้ใช้งานระบบของบริษัทฯ (Application System) และระดับผู้ดูแลระบบงานของบริษัทฯ (Administrator) ที่อยู่ในระดับ Application มีการกำหนดรหัสผ่าน ดังนี้

(1) อายุของรหัสผ่านใช้ได้ไม่เกิน 90 วัน หรือ 3 เดือน

(2) ความยาวรหัสผ่านอย่างน้อย 6 ตัวอักษร

(3) ความซับซ้อนของรหัสผ่าน กำหนดให้ต้องประกอบด้วย ตัวเลข ตัวอักษรภาษาอังกฤษ ทั้งที่เป็นตัวใหญ่และตัวเล็ก

(4) จำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 5 ครั้ง

(5) จำนวนครั้งที่ไม่ให้กำหนดรหัสผ่านซ้ำกับรหัสผ่านเดิม 3 ครั้ง

5.2 ระดับระบบปฏิบัติการ (Operating System) ในส่วนของ Application บน Server

ในส่วนของ Application ต้องติดตั้งอยู่บนพื้นฐานของระบบปฏิบัติการ OS บน Server ที่มีความสำคัญต่อการทำงานโดยตรง เช่น CentOS และ Ubuntu ไม่ได้กำหนดอายุของรหัสผ่าน เนื่องจากระบบปฏิบัติการพื้นฐานเหล่านี้จะต้องมีการใช้งานร่วมกับ Application ที่มีการเชื่อมต่อกับฐานข้อมูลหลักอยู่ตลอดเวลา และมีผู้ที่มีสิทธิในการเข้าถึงเพื่อบริหารจัดการและควบคุม เครื่องคอมพิวเตอร์แม่ข่ายให้สามารถใช้งานได้อย่างต่อเนื่อง ไม่หยุดชะงัก ทั้งนี้ได้ประเมินแล้วว่าจะไม่เป็นความเสี่ยงต่อความปลอดภัยของการเข้าถึงระบบ เนื่องจากผู้มีสิทธิในการเข้าถึงจะต้องได้รับหมอบหมายจากผู้จัดการฝ่ายสารสนเทศเท่านั้น แต่มีข้อกำหนดในการตั้งรหัสผ่านเพื่อเข้าใช้งานดังนี้

(1) ความยาวรหัสผ่านอย่างน้อย 8 ตัวอักษร

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

(3) จำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 5 ครั้ง

(4) จำนวนครั้งที่ไม่ให้กำหนดรหัสผ่านซ้ำกับรหัสผ่านเดิม 3 ครั้ง

5.3 ระดับระบบฐานข้อมูล Database และ ระบบปฏิบัติการ OS บน Server

ระบบฐานข้อมูล (Database) ของบริษัทฯ ไม่มีการกำหนดอายุของรหัสผ่านในการเข้าถึงข้อมูล เนื่องจากมี Application ต่างๆ เชื่อมต่อกับระบบฐานข้อมูล เพื่อทำการอ่านและเขียนข้อมูลตลอดเวลา หาก Password ที่ใช้งานในระบบนี้มีการเปลี่ยนแปลง ก็จะต้องทำการแก้ไขหรือปรับปรุง Application ด้วยทุกครั้ง (ทั้งนี้ ได้ประเมินแล้วว่าจะไม่เป็นความเสี่ยงต่อความปลอดภัยของข้อมูลและฐานข้อมูล เนื่องจากผู้ใช้งานไม่สามารถเข้าถึงฐานข้อมูลได้โดยตรง) สำหรับบัญชีผู้ใช้งานสิทธิสูง ซึ่งได้แก่บัญชี Root ของระบบปฏิบัติการและระบบฐานข้อมูลกำหนดสิทธิให้ผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายเป็นผู้ดูแลรับผิดชอบ

5.4 การเข้าใช้งานผ่านระบบเครือข่ายส่วนบุคคลเสมือน (Virtual Private Network (VPN))

การเข้าใช้งานเพื่อเชื่อมต่อฐานข้อมูลของบริษัทฯ และระบบปฏิบัติการ OS บนเครื่อง Server จากภายนอก ผู้ที่ทำการเชื่อมต่อต้องได้รับอนุญาตจากผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายสารสนเทศ หรือผู้มีอำนาจสูงกว่า ในการเข้าเชื่อมต่อเพื่อใช้งานฐานข้อมูลผ่านระบบเครือข่ายส่วนบุคคลเสมือน (Virtual Private Network (VPN)) หรือระบบเครือข่ายภายใน (Local Area Network (LAN)) เท่านั้น โดยผู้ใช้งานจะต้อง Login ด้วย Username และ Password ของตนเองก่อนทุกครั้ง

5.5 การขออนุมัติ การอนุญาตให้เข้าใช้งาน การเปลี่ยนตำแหน่งโยกย้าย หรือสิ้นสุดการจ้าง และการระงับการเข้าใช้งานในระบบสารสนเทศที่มีความสำคัญจะต้องมีบันทึกเก็บไว้เป็นหลักฐานเสมอ

5.6 การใช้งานระบบสารสนเทศอื่น ๆ เช่น จดหมายอิเล็กทรอนิกส์ หรือเว็บไซต์ อนุญาตให้ใช้บัญชีรายชื่อแบบกลุ่มได้ตามความเหมาะสมและลักษณะการใช้งาน เช่น สาขา หน่วย หรือส่วนงานในสำนักงานใหญ่ เป็นต้น เพื่อไม่ให้เป็นอุปสรรคต่อการทำงาน

5.7 การกำหนดชื่อผู้ใช้งาน (Username) ให้กำหนดเป็นชื่อภาษาอังกฤษด้วยตัวอักษรพิมพ์ใหญ่ หรือตัวอักษรพิมพ์เล็กให้ตรงกับชื่อในบัตรประชาชนของผู้ใช้งาน หากซ้ำกับชื่อผู้ใช้งานที่มีอยู่แล้ว ให้ตามด้วยตัวเลขหรือตัวอักษรแรกของนามสกุล หากยังซ้ำกันให้เพิ่มตัวอักษรตัวที่สองจากนามสกุล (หรือเพิ่มตัวอักษรในลำดับถัดไป) จนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น หากเป็นส่วนงานในพื้นที่ให้กำหนดชื่อผู้ใช้งานโดยใช้เลขรหัสของส่วนงาน เช่น SAK0100 หรือใช้ชื่อภาษาอังกฤษของส่วนงานในสำนักงานใหญ่ เช่น Finance หรือ Internal Audit เป็นต้น

6. หน้าที่ ความรับผิดชอบของผู้บริหาร

6.1 ชี้แจงให้ผู้ใช้งานสารสนเทศทราบถึงนโยบาย มาตรฐาน กรอบดำเนินงาน ขั้นตอนการปฏิบัติ วิธีปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

6.2 ดูแล แนะนำ ตักเตือน กรณีพบเห็นการปฏิบัติไม่ถูกต้องหรือไม่เหมาะสมเกี่ยวกับการใช้งานระบบสารสนเทศและเครือข่ายสื่อสารข้อมูล

6.3 พิจารณาลงโทษทางวินัยแก่ผู้กระทำความผิดอย่างเสมอภาค และเป็นธรรม

7. หน้าที่ ความรับผิดชอบ และมารยาทในการใช้งานระบบสารสนเทศของผู้ใช้งาน (Users Duties, Responsibilities and Etiquette)

7.1 ผู้ใช้งานระบบสารสนเทศต้องเรียนรู้ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติ วิธีปฏิบัติ คำแนะนำและกระบวนการต่างๆ ของบริษัทฯ เกี่ยวกับการใช้งานระบบสารสนเทศและเครือข่ายการสื่อสารที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

7.2 ผู้ใช้งานระบบสารสนเทศ มีหน้าที่เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีเมื่อเข้าใช้งานเป็นครั้งแรก ตั้งรหัสผ่านใหม่ที่คาดเดาได้ยาก รักษาความลับของรหัสผ่าน และเปลี่ยนรหัสผ่านใหม่ทุก 90 วัน หรือเมื่อผู้ใช้เห็นสมควรต้องเปลี่ยนรหัสผ่าน และต้องเก็บรักษารหัสผ่านและรหัสอื่นใดที่บริษัทฯกำหนด เพื่อใช้ในการเข้าถึงระบบสารสนเทศ หรือข้อมูลของบริษัทฯ เป็นความลับส่วนตัวของผู้ใช้งานระบบ ซึ่งจะเก็บรักษาไว้มิให้ผู้อื่นรู้ และห้ามใช้ร่วมกับผู้อื่น ห้ามตั้งรหัสผ่านซ้ำกับรหัสเก่า ห้ามตั้งรหัสผ่านที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือห้ามตั้งรหัสผ่านซ้ำกันในทุกระบบที่ผู้ใช้มีสิทธิใช้งาน

7.3 การทำสำเนาข้อมูลต่าง ๆ ให้เป็นไปตามข้อกำหนด ระเบียบการรักษาความมั่นคงความปลอดภัยไซเบอร์ของบริษัทฯ

7.4 ผู้ใช้งานมีหน้าที่เรียนรู้การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์พ่วงต่ออย่างถูกวิธี และช่วยดูแลอุปกรณ์ที่ตนใช้งานเป็นประจำหรือได้รับมอบหมายให้ดูแลให้ใช้งานได้เป็นปกติ เช่น ทำความสะอาด คอยสังเกตสัญญาณหรือไฟเตือน และสังเกตการทำงานที่ผิดปกติของอุปกรณ์ และควรตรวจเช็คการทำงานของฮาร์ดดิสก์และระบบไฟล์ข้อมูล (File System) โดยสม่ำเสมออย่างน้อยทุก 6 เดือน

7.5 ผู้ใช้งานต้องไม่ถอดถอน หยุดการทำงาน หรือดัดแปลงซอฟท์แวร์/โปรแกรมที่ติดตั้งไว้โดยผู้ดูแลระบบ โดยเฉพาะโปรแกรมแอนติไวรัส แอนติมัลแวร์ เพราะเป็นสาเหตุและความเสี่ยงที่จะทำให้เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกติ หากไม่แน่ใจให้สอบถามกับผู้ดูแลระบบก่อน

7.6 ผู้ใช้งานต้องไม่ดาวน์โหลดซอฟท์แวร์/โปรแกรมที่ไม่ได้รับการรับรอง ไม่มีลิขสิทธิ์ที่ถูกต้อง หรือมีความเสี่ยงต่อไวรัสและมัลแวร์ มาติดตั้งบนเครื่องคอมพิวเตอร์ที่ตนใช้งาน และควรใช้ความระมัดระวังในการเข้าเว็บไซต์บนอินเตอร์เน็ต ไม่คลิกปุ่มใด ๆ ที่แสดงบนหน้าจอโดยการคาดเดา

7.7 ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ของบริษัทฯ ไปใช้ท่องเว็บไซต์ที่ไม่มีประโยชน์กับการทำงาน เว็บไซต์ที่มีลักษณะต้องห้ามทางศีลธรรม ขัดต่อความสงบเรียบร้อย ขัดต่อกฎหมาย และเว็บไซต์ที่อาจมีความเสี่ยงต่อไวรัสและมัลแวร์ เช่น เล่นพนันออนไลน์ เล่นเกมออนไลน์ ดูหนังหรือภาพลามกอนาจร การดาวน์โหลดไฟล์จากแหล่งที่ไม่รู้ที่มา เป็นต้น

7.8 ในเวลางาน ผู้ใช้งานต้องไม่ใช้อุปกรณ์และเครือข่ายสื่อสารของบริษัทฯ เข้าชมหรือดาวน์โหลดไฟล์มัลติมีเดียขนาดใหญ่ เช่น การดูคลิป ดูหนัง ฟังเพลง ดูการถ่ายทอดกีฬา เป็นต้น ซึ่งไม่เป็นประโยชน์กับการทำงาน เพราะเป็นการใช้ทรัพยากรเครือข่ายโดยไม่เหมาะสม และอาจส่งผลกระทบต่อการปฏิบัติงานของเพื่อนร่วมงาน

7.9 ผู้ใช้งานต้องไม่นำไฟล์ข้อมูลส่วนตัว เช่น เพลง รูปภาพ คลิป ซึ่งมีเนื้อหาที่ไม่เป็นประโยชน์ในการทำงานมาเก็บไว้ในเครื่องคอมพิวเตอร์ของบริษัทฯ

7.10 ผู้ใช้งานต้องไม่จัดเก็บ ไม่เปิดเสียงและภาพที่มีลักษณะขัดต่อศีลธรรม ผิดกฎหมาย สิ่งลามกอนาจาร และสื่อที่อาจทำให้เกิดความรู้สึกอึดอัดไม่สบายใจแก่เพื่อนร่วมงาน เช่น ความเห็นทางการเมืองและลัทธิความเชื่อทางศาสนา เป็นต้น

7.11 ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ เครื่องพิมพ์ เครื่องถ่ายเอกสาร แฟกซ์ และอุปกรณ์สารสนเทศที่เป็นทรัพย์สินของบริษัทฯ โดยเฉพาะสิ่งที่เป็นวัสดุสิ้นเปลืองไปใช้ในเรื่องส่วนตัว และควรนำของส่วนตัวมาใช้เพื่อการดังกล่าว

7.12 ผู้ใช้งานต้องดูแลให้เครื่องคอมพิวเตอร์ได้รับการจ่ายไฟจากเครื่องสำรองไฟ UPS และดูแลให้เครื่องสำรองไฟ UPS ยังสำรองไฟไว้ได้เมื่อไฟตก (แบตเตอรี่ของ UPS จะมีอายุการใช้งานโดยเฉลี่ย 1.5-2 ปี) เมื่อเครื่องสำรองไฟไม่ทำงานจะต้องรีบเปลี่ยนแบตเตอรี่หรือเปลี่ยนเครื่องสำรองไฟโดยทันที เพราะเป็นความเสี่ยงที่จะทำให้ฮาร์ดดิสก์และข้อมูลที่เก็บไว้เสียหายจนใช้การไม่ได้

7.13 หากเครื่องคอมพิวเตอร์หรืออุปกรณ์พ่วงต่อที่ใช้งานมีปัญหา ให้ปรึกษากับผู้ดูแลระบบหรือส่งคืนสำนักงานใหญ่เพื่อเบิกของนำไปใช้ทดแทน ไม่ควรนำไปซ่อมเองโดยพลการเพราะมักจะแก้ปัญหาไม่จบ ทำให้เสียเงินและเวลาโดยใช่เหตุ

7.14 ผู้ใช้งานต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

7.15 ผู้ใช้งานต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าใช้งาน

7.16 ให้ความร่วมมือกับบริษัทฯ อย่างเต็มที่ในการป้องกันระบบสารสนเทศและระบบเครือข่ายการสื่อสารข้อมูลของบริษัทฯ โดยแจ้งให้บริษัทฯ ทราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม หรือหากพบเห็นการบุกรุก โจรกรรมทำลาย แทรกแซงการทำงาน หรือการกระทำที่อาจสร้างความเสียหายต่อบริษัทฯ

8. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (Duties and Responsibilities of System Administrators)

8.1 บริษัทมีหน้าที่จัดหาเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์พ่วงต่อที่มีคุณสมบัติเหมาะสมให้กับพนักงาน และมีหน้าที่ติดตั้งระบบปฏิบัติการ ซอฟต์แวร์ และโปรแกรมประยุกต์ให้พร้อมสำหรับการใช้งาน รวมถึงมีหน้าที่ซ่อมแซม จัดหาอะไหล่ ให้คำปรึกษาในการใช้งานและการซ่อมบำรุงแก่ผู้ใช้งาน

8.2 ให้ผู้ดูแลระบบมีหน้าที่ควบคุมสิทธิในการเข้าใช้งานระบบสารสนเทศของผู้ใช้งาน สิทธิในการเข้าใช้งานได้แก่ (1) ให้อ่านอย่างเดียว (2) ให้สร้างข้อมูลได้ (3) ให้แก้ไขข้อมูลได้ (4) ให้อนุมัติได้ (5) ไม่มีสิทธิใช้งานตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

8.3 ผู้ใช้งานที่จะเข้าใช้งานระบบสารสนเทศได้ จะต้องเป็นไปตามนโยบายที่บริษัทฯ กำหนด หรือได้รับอนุญาตจากกรรมการผู้จัดการ หรือรองกรรมการผู้จัดการ หรือผู้จัดการฝ่ายสารสนเทศ และให้มีการทบทวนสิทธิผู้ใช้งานในระบบงานต่าง ๆ ได้แก่ ระบบงานสินเชื่อ LMIS, ระบบงานสินเชื่อเช่าซื้อ HPS, และระบบงานบัญชี SAP อย่างน้อยปีละ 1 ครั้ง

8.4 ระบบสารสนเทศทุกระบบจะต้องมีการกำหนดและมอบหมายหน้าที่ในการดูแลระบบ (System Administration) ให้กับผู้ดูแลระบบ (System Administrator) และจัดทำกรอบหน้าที่ไว้อย่างชัดเจน

8.5 หน้าที่ของผู้ดูแลระบบ (System Administrator) ต้องประกอบด้วยเรื่องต่อไปนี้เป็นอย่างน้อย

8.5.1 จัดทำบัญชีรายชื่อผู้ใช้งาน

8.5.2 ตั้งหรือเปลี่ยนรหัสผ่าน

8.5.3 รักษาความปลอดภัยในการเข้าถึงและใช้งานระบบให้เป็นไปตามนโยบายของบริษัทฯ

8.5.4 ทำการสำรองข้อมูลและทดสอบการเรียกคืนข้อมูลในระบบตามระยะเวลาที่กำหนด

8.5.5 ตรวจสอบสภาวะการทำงานของระบบอย่างสม่ำเสมอ

8.5.6 รับผิดชอบในการแก้ไขปัญหาเพื่อให้ระบบสารสนเทศทำงานได้เป็นปกติ

8.5.7 ให้คำปรึกษาแก่ผู้ใช้งาน

8.5.8 ควบคุมดูแลบุคคลภายนอกที่เกี่ยวข้องกับการใช้ระบบสารสนเทศ

9. การใช้งานระบบเครือข่ายสื่อสาร

9.1 กำหนดให้อุปกรณ์เครือข่าย เซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์พ่วงต่อทุกชิ้นที่อยู่บนเครือข่ายสื่อสารของสำนักงานใหญ่ มีการกำหนดหมายเลขไอพีแอดเดรส (IP Address) แบบค่าคงที่ (Static) และมีการทำทะเบียนหมายเลขไอพีไว้ เพื่อสามารถใช้ในการตรวจสอบได้

9.2 การเปิดใช้งานไฟร์วอลล์ (Firewall) และควบคุมการเปิดพอร์ต (Port) กำหนดนโยบายให้มีการเปิดใช้งานเท่าที่จำเป็นเท่านั้น และให้ทำทะเบียนพอร์ตที่เปิดใช้งานไว้

9.3 ห้ามมิให้พนักงานนำอุปกรณ์เครือข่ายมาติดตั้งเองโดยพลการ การติดตั้งอุปกรณ์เครือข่าย เช่น เราเตอร์ (Router) ไวไฟเราเตอร์ (Wifi Router) แอคเซสพอยต์ (Access Point) สวิตช์ (Switch) ในสำนักงานใหญ่ จะต้อง

ได้รับการอนุญาตจากผู้ดูแลระบบเสียก่อน ทั้งนี้ เพื่อป้องกันความเสียหายและอาจจะเกิดการรบกวนต่อการทำงานของระบบเครือข่าย

10. การรักษาความลับของข้อมูล (Secrecy of Data)

10.1 ห้ามมิให้พนักงานเปิดเผย เผยแพร่แก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้อง หรือทำสำเนาโยกย้ายออกสู่ภายนอกซึ่งข้อมูลที่เป็นความลับที่อยู่ในระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด

10.2 ข้อมูลที่เป็นความลับประกอบด้วย

(1) ข้อมูลและรายงานทางบัญชี

(2) ข้อมูลและรายงานทางการเงิน

(3) งบประมาณ

(4) ข้อมูลประวัติและรายได้ของพนักงาน

(5) นโยบายหรือคำสั่งที่ยังไม่ได้รับอนุญาตให้ทำการเผยแพร่

(6) ยุทธศาสตร์และแผนธุรกิจ

(7) ข้อมูลส่วนบุคคลและประวัติการทำสินเชื่อของลูกค้า และข้อมูลที่เชื่อมโยงกับรายการดังกล่าวข้างต้น เช่น ข้อมูลเชิงวิเคราะห์ต่าง ๆ เป็นต้น

10.3 การแลกเปลี่ยนข้อมูลที่เป็นความลับ ให้ผู้จัดทำและเจ้าของข้อมูลจัดเก็บไว้ในพื้นที่ส่วนตัวเท่านั้น หากมีความจำเป็นจะต้องแลกเปลี่ยน ข้อมูลที่เป็นความลับ ด้วยวิธีการทางอิเล็กทรอนิกส์ ให้เจ้าของข้อมูลทำการเข้ารหัสไฟล์ข้อมูลเพื่อป้องกันการเปิดอ่านโดยบุคคลอื่น แจ้งรหัสสำหรับเปิดอ่านไฟล์ให้กับผู้รับข้อมูล และลบไฟล์ออกจากพื้นที่แลกเปลี่ยนข้อมูลเมื่อผู้รับได้รับข้อมูลแล้ว ซึ่งจะต้องสอดคล้องกับระเบียบวิธีปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ

11. ห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) และการติดตั้งอุปกรณ์ (Equipment Installation)

11.1 เครื่องเซิร์ฟเวอร์ (Server) และอุปกรณ์เครือข่าย (Network Equipment) ที่เป็นส่วนประกอบของระบบสารสนเทศของบริษัทฯ ให้ติดตั้งในห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) หรือในสถานที่เฉพาะที่กำหนดไว้และอนุญาตให้เข้าถึงได้เฉพาะผู้มีหน้าที่เกี่ยวข้องเท่านั้น

11.2 การเข้าไปปฏิบัติงานในห้องอุปกรณ์เซิร์ฟเวอร์ จะต้องมีการบันทึกไว้ในสมุดบันทึกทุกครั้ง พร้อมรายละเอียดได้แก่ ชื่อ เวลาเข้า-ออก เรื่องที่เข้าไปดำเนินการ และลายมือชื่อ หากเป็นบุคคลภายนอกจะต้องมีลายมือชื่อของผู้กำกับงานของบริษัทฯ ร่วมอยู่ด้วยทุกครั้ง

11.3 ห้องอุปกรณ์เซิร์ฟเวอร์ (Server Room) ต้องมีการควบคุมอุณหภูมิ ความชื้น และฝุ่นละอองไว้อย่างเหมาะสมตลอดเวลา และควรจัดให้มีระบบแจ้งเตือนเมื่อมีความผิดปกติเกิดขึ้น

11.4 เครื่องเซิร์ฟเวอร์และอุปกรณ์เครือข่าย ให้ติดตั้งและจัดวางในตู้อุปกรณ์ (Rack) การเดินสายสัญญาณให้จัดวางด้วยความเป็นระเบียบเรียบร้อย และให้จัดทำป้ายชื่อ (Label) และแผนผัง (Diagram) การเดินสายสัญญาณและผังการเชื่อมต่ออุปกรณ์เครือข่าย

11.5 ให้ทำป้ายชื่อกำกับติดไว้บนเครื่องเซิร์ฟเวอร์ อุปกรณ์เครือข่าย สายสัญญาณ ร่วมกับการพิจารณาใช้สายสัญญาณที่มีสีแตกต่างกัน เพื่อป้องกันการเชื่อมต่อสายสัญญาณผิดเส้น

12. การป้องกันการหยุดชะงักของระบบ (Fault Tolerance)

12.1 เครื่องเซิร์ฟเวอร์ของระบบสารสนเทศจะต้องติดตั้งฮาร์ดดิสก์จำนวนอย่างน้อย 2 ลูก และตั้งให้มีการทำงานซ้ำซ้อนกัน (Redundancy) อย่างน้อยในแบบ RAID 1, 5, 6, 10 หรือในแบบอื่นที่เทียบเท่ากันหรือดีกว่า เพื่อป้องกันความเสียหายที่จะเกิดกับข้อมูลในกรณีที่ฮาร์ดดิสก์ลูกใดลูกหนึ่งเสียอย่างกะทันหัน

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

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

12.4 เครื่องเซิร์ฟเวอร์และอุปกรณ์เครือข่ายจะต้องได้รับการจ่ายไฟจากเครื่องสำรองไฟ (UPS) เท่านั้น เพื่อป้องกันไม่ให้การทำงานหยุดชะงักเมื่อไฟตกหรือไฟดับ และป้องกันความเสียหายที่อาจเกิดขึ้นได้กับฮาร์ดดิสก์ (Hard Disk) และระบบไฟล์ข้อมูล (File System) จากเหตุดังกล่าว

12.5 เครื่องสำรองไฟของระบบสารสนเทศควรสำรองไฟได้ไม่น้อยกว่า 30 นาที เพื่อให้ผู้ดูแลระบบมีเวลามากพอในการดำเนินการปิดระบบ (Shutdown) อย่างเป็นขั้นตอน เพื่อป้องกันข้อมูลสูญหายและความเสียหายที่อาจจะเกิดขึ้นกับฮาร์ดดิสก์ (Hard Disk) หรือระบบไฟล์ (File System) หรือระบบฐานข้อมูล (Database)

12.6 ตั้งค่าให้เครื่องเซิร์ฟเวอร์ปิดตัวเอง (Shutdown) ได้โดยอัตโนมัติ เมื่อพบว่ามีการจ่ายไฟจากแบตเตอรี่ของเครื่องสำรองไฟนานเกินกว่า 30 นาที

12.7 จัดให้มีเครื่องกำเนิดไฟฟ้าสำรอง (Generator) เพื่อจ่ายไฟให้กับอุปกรณ์และระบบควบคุมอุณหภูมิในห้องเซิร์ฟเวอร์ได้โดยอัตโนมัติภายในเวลาไม่เกิน 5 นาที เมื่อระบบจ่ายไฟหลักหยุดการจ่ายไฟ และจ่ายไฟได้อย่างต่อเนื่องและเพียงพอจนกว่าจะได้รับการจ่ายไฟเป็นปกติ

12.8 จัดให้มีช่องทางสำรองในการเชื่อมต่อกับอินเตอร์เน็ตในกรณีที่ช่องทางหลักไม่สามารถใช้การได้

13. การสำรองข้อมูลและการเรียกคืน (Backup and Recovery)

13.1 ระบบสารสนเทศที่มีการเพิ่ม เปลี่ยนแปลง หรือแก้ไขข้อมูลเป็นประจำทุกวัน ให้มีการสำรองข้อมูลในระบบทุกวัน (รายละเอียดตามเอกสารแนบ)

13.2. ระบบสารสนเทศที่มีการเพิ่ม เปลี่ยนแปลง หรือแก้ไขข้อมูลเป็นประจำทุกสัปดาห์หรือทุกเดือน ให้มีการสำรองข้อมูลในระบบตามรอบระยะเวลาดังกล่าว ระบบที่อยู่ในข่ายดังกล่าว ได้แก่

(1) ระบบงานบัญชีเงินเดือนและระบบงานบุคคล

(2) ระบบเผยแพร่ข้อมูลจากเว็บไซต์ เป็นต้น

13.3 ข้อมูลจากระบบสารสนเทศที่จะต้องมีการทำสำรอง ได้แก่ ข้อมูลของผู้ใช้งาน (User Data) ข้อมูลการติดตั้งและปรับแต่งระบบ (Configuration Files) และข้อมูลอื่น ๆ ที่เกี่ยวกับผู้ใช้งาน โดยข้อมูลที่สำรองไว้ ให้แยกเก็บไว้ต่างหากจากเครื่องเซิร์ฟเวอร์ที่กำลังใช้งาน

13.4 ในกรณีที่ระบบสารสนเทศระบบใดระบบหนึ่งเกิดการล้มเหลวโดยกะทันหัน จะต้องมีระบบสำรองหรือวิธีการที่ทำให้สามารถเรียกคืนการทำงานได้ภายในระยะเวลา 4 ชั่วโมง

13.5 ให้มีการทบทวนและทดสอบการสำรองข้อมูลและการเรียกคืนข้อมูลจากระบบสารสนเทศที่ใช้ปฏิบัติการให้เป็นไปตามนโยบายข้างต้น อย่างน้อยปีละ 1 ครั้ง

14. การเก็บบันทึกประวัติการเข้าใช้งาน (Logging)

ให้มีการจัดเก็บบันทึกประวัติการเข้าใช้งาน (Login) ประวัติการใช้งาน (Usage) ในระบบที่สำคัญ รวมถึงการแก้ไข เพิ่ม หรือลบข้อมูลให้เป็นไปตามข้อกำหนดของกฎหมาย

15. ระบบแจ้งเตือนสถานะการทำงาน (Monitoring)

จะต้องจัดให้มีการแจ้งเตือนสถานะการทำงาน (Monitoring) ของระบบเครือข่ายและเครื่องเซิร์ฟเวอร์ของระบบสารสนเทศ โดยผู้ดูแลระบบสามารถตรวจสอบสถานการณ์ทำงานและการแจ้งเตือนได้จากระยะทางไกล

16. คู่มือการใช้งานและดูแลระบบสารสนเทศ (Documentation)

16.1 ให้จัดทำคู่มือการใช้งาน การติดตั้ง การดูแลรักษา การสำรองและเรียกคืนข้อมูล ของระบบสารสนเทศ โดยให้มีรายละเอียดที่จำเป็นสำหรับการดูแลรักษาระบบอย่างครบถ้วน เพียงพอ และอ่านเข้าใจได้อย่างชัดเจน

16.2 ให้มีการจัดทำทะเบียนระบบสารสนเทศ ประกอบด้วยข้อมูลที่สำคัญของแต่ละระบบ ได้แก่ ชื่อระบบ บริการของระบบโดยสังเขป กลุ่มผู้ใช้งาน คุณลักษณะของเซิร์ฟเวอร์ (ยี่ห้อและรุ่น ซีพียู จำนวนหน่วยความจำ ฮาร์ดดิสก์และความจุ) ระบบปฏิบัติการที่ติดตั้ง ซอฟท์แวร์ที่ติดตั้ง การตั้งค่าต่าง ๆ ของระบบ (Configuration) ไอพีแอดเดรส (IP Address) แผนภาพแสดงลักษณะโครงสร้าง ชื่อบัญชีผู้ดูแลระบบ (รหัสผ่านให้แจ้งต่างหาก) ชื่อและข้อมูลติดต่อของผู้ดูแลระบบ ผู้จัดทำทะเบียน วันที่ที่จัดทำทะเบียน เป็นต้น

16.3 ทะเบียนระบบสารสนเทศจะต้องได้รับการทบทวนปรับปรุงตามระยะเวลาที่กำหนด อย่างน้อยปีละ 1 ครั้ง

16.4 ให้รวบรวมและจัดเก็บข้อมูลคุณลักษณะของอุปกรณ์ (Specification) และคู่มือการใช้งาน (Manual) ของทั้งฮาร์ดแวร์และซอฟท์แวร์ของระบบสารสนเทศ ในรูปแบบไฟล์อิเล็กทรอนิกส์ เก็บไว้อย่างน้อย 1 ชุด

17. การบำรุงรักษาและการสำรองอะไหล่ (Spare Parts)

ให้ประเมินความเหมาะสมของเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์พ่วงต่อ ระบบปฏิบัติการ ซอฟท์แวร์และโปรแกรมประยุกต์ ที่มีการใช้งานในบริษัทฯ ตามประสิทธิภาพการทำงาน อายุการ

ใช้งาน ความเหมาะสมในการใช้งาน ค่าใช้จ่ายในการซ่อมบำรุงและการสำรองอะไหล่ เพื่อจัดตั้งงบประมาณในการจัดซื้อจัดหาอุปกรณ์ใหม่มาใช้งานทดแทน อย่างน้อยปีละ 1 ครั้ง

18. ขั้นตอนปฏิบัติการจัดการบัญชีผู้ใช้งานในระบบงาน LMIS, HPS, SAP

18.1 ข้อปฏิบัติในการเพิ่ม/เปลี่ยนแปลง/ระงับ สิทธิการใช้งานในระบบ LMIS และ HPS

18.1.1 การเพิ่มสิทธิให้กับพนักงานใหม่

1) ฝ่ายสารสนเทศ รับคำสั่งการเพิ่มพนักงานทดลองงานจากฝ่ายบุคคล ที่ได้รับการอนุมัติจากกรรมการผู้จัดการ
2) ฝ่ายสารสนเทศเพิ่มข้อมูล ชื่อ-สกุล ตำแหน่ง และสังกัดสาขา หน่วยในระบบให้ถูกต้อง
3) ฝ่ายสารสนเทศเพิ่มชื่อผู้ใช้งาน และรหัสผ่าน รวมถึงสิทธิการใช้งานและการเข้าถึงข้อมูลให้เป็นไปตามตำแหน่งงาน
4) ผู้จัดการฝ่ายสารสนเทศหรือหัวหน้าฝ่ายสารสนเทศตรวจสอบการเพิ่มข้อมูลพนักงานและสิทธิการใช้งานและการเข้าถึงข้อมูลในระบบ
5) ฝ่ายสารสนเทศแจ้งข้อมูลชื่อผู้ใช้งานและรหัสผ่านให้พนักงานทดลองงานทราบในวันแรกของการทำงาน

18.1.2 การเปลี่ยนแปลงสิทธิในระบบกรณีมีการโยกย้ายหรือเปลี่ยนตำแหน่งงาน

1) ฝ่ายสารสนเทศรับคำสั่งการเปลี่ยนแปลงตำแหน่ง หรือโยกย้ายสถานที่ทำงานจากฝ่ายบุคคล ที่ได้รับการอนุมัติจากกรรมการผู้จัดการ
2) ฝ่ายสารสนเทศดำเนินการเปลี่ยนแปลงหรือโยกย้ายพนักงานในระบบตามคำสั่งที่ได้รับอนุมัติ
3) ฝ่ายสารสนเทศปรับปรุงสิทธิการเข้าใช้งานในระบบตามตำแหน่งงาน
4) ผู้จัดการฝ่ายสารสนเทศหรือหัวหน้าฝ่ายสารสนเทศตรวจสอบการเปลี่ยนแปลง หรือโยกย้าย และการกำหนดสิทธิในระบบ

18.1.3 การระงับ หรือ disable บัญชีรายชื่อผู้ใช้งานในระบบถกรณีพนักงานลาออก หรือมีคำสั่งให้พักงานหรือออกจากการเป็นพนักงาน

1) ฝ่ายสารสนเทศรับคำสั่งพนักงานลาออก หรือพักงาน หรือให้ออกจากฝ่ายบุคคลที่ได้รับอนุมัติจากกรรมการผู้จัดการ
2) ฝ่ายสารสนเทศระงับสิทธิการใช้งานในระบบของพนักงานคนดังกล่าว
3) ผู้จัดการฝ่ายสารสนเทศหรือหัวหน้าฝ่ายสารสนเทศตรวจสอบการระงับสิทธิในระบบ
4) ฝ่ายสารสนเทศบันทึกยืนยันการระงับสิทธิผู้ใช้งาน ในเอกสารใบลาออกที่ได้รับจากฝ่ายบุคคล
5) ฝ่ายสารสนเทศบันทึกทะเบียนคุมพนักงานลาออกไว้เป็นลายลักษณ์อักษร

18.1.4 กรณีมีการขอเปลี่ยนแปลง เพิ่ม/ลบสิทธิการใช้งานในบางเมนูงาน

1) หัวหน้างานในส่วนงานที่ต้องการปรับเปลี่ยนสิทธิการเข้าใช้งานในระบบจะต้องทำบันทึกขอการเปลี่ยนแปลงสิทธิการใช้งานในระบบของพนักงานในสังกัดถึงกรรมการผู้จัดการหรือรองกรรมการผู้จัดการพิจารณาอนุมัติ
2) กรรมการผู้จัดการ หรือรองกรรมการผู้จัดการพิจารณาอนุมัติการเปลี่ยนแปลงสิทธิ
3) ฝ่ายสารสนเทศดำเนินการเปลี่ยนแปลงสิทธิในระบบงาน
4) ผู้จัดการฝ่ายสารสนเทศหรือหัวหน้าฝ่ายสารสนเทศตรวจสอบการเปลี่ยนแปลงสิทธิในระบบงาน
5) ฝ่ายสารสนเทศแจ้งผลการดำเนินการเปลี่ยนแปลงให้ผู้ร้องขอทราบเพื่อเข้าใช้งานในระบบ

18.1.5 ทุกสิ้นเดือนฝ่ายสารสนเทศสรุปรายงานการ/เปลี่ยนแปลง/ระงับสิทธิการใช้งานในระบบ LMIS ระบบ HPS และเปรียบเทียบบัญชีรายชื่อผู้ใช้งานในระบบให้ตรงกับข้อมูลพนักงานจากฝ่ายบุคคล

18.2 ข้อปฏิบัติในการเพิ่ม/เปลี่ยนแปลง/ระงับสิทธิการใช้งานในระบบ SAP จะกระทำได้ก็ต่อเมื่อกรรมการผู้จัดการ หรือรองกรรมการผู้จัดการพิจารณาอนุมัติให้มีการปรับเปลี่ยนสิทธิการเข้าใช้งานดังกล่าวตามความเหมาะสม หรือตามตำแหน่ง โดยมีข้อปฏิบัติดังนี้

18.2.1 หัวหน้างานในส่วนงานที่ต้องการปรับเปลี่ยนสิทธิการเข้าใช้งานในระบบ SAP ของพนักงานในสังกัดจะต้องทำบันทึกขอการเปลี่ยนแปลงสิทธิ SAP เสนอต่อกรรมการผู้จัดการ หรือรองกรรมการผู้จัดการพิจารณาอนุมัติ

18.2.2 กรรมการผู้จัดการ หรือรองกรรมการผู้จัดการ พิจารณาอนุมัติการเปลี่ยนแปลง

18.2.3 ฝ่ายสารสนเทศปรับปรุง/แก้ไข/ระงับสิทธิในระบบ SAP

18.2.4 ผู้จัดการฝ่ายสารสนเทศหรือหัวหน้าฝ่ายสารสนเทศตรวจสอบการเปลี่ยนแปลงสิทธิในระบบงาน

18.2.5 ฝ่ายสารสนเทศแจ้งผลการเปลี่ยนแปลงให้ผู้ร้องขอทราบเพื่อเข้าใช้งานในระบบ

19. ขั้นตอนปฏิบัติในการเปลี่ยนแปลง แก้ไข และการพัฒนาระบบสารสนเทศ

19.1 ขั้นตอนการพัฒนาระบบงานสารสนเทศตามแผนงานและโครงการประจำปี

19.1.1 ฝ่ายสารสนเทศจัดทำแผนโครงการ และรายละเอียดการพัฒนาเสนอต่อกรรมการผู้จัดการพิจารณาอนุมัติโครงการ

19.1.2 จัดทำรายละเอียดขออนุมัติแก้ไข/ปรับปรุงระบบตามแผนงานโครงการที่ได้รับอนุมัติ

19.1.3 ดำเนินการส่งเอกสารรายละเอียดให้ผู้พัฒนาระบบแก้ไข/ปรับปรุงระบบ

19.1.4 ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบทดสอบ (Development System)

19.1.5 ฝ่ายสารสนเทศและผู้ใช้งานตรวจสอบข้อมูลในระบบทดสอบ

19.1.6 ฝ่ายสารสนเทศยืนยันความถูกต้องของโปรแกรม และแจ้งให้ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบ (Production System)

19.1.7 ฝ่ายสารสนเทศติดตามประเมินผลการแก้ไขเปลี่ยนแปลงหลังจากมีการปรับปรุง

19.2 ขั้นตอนการแก้ไขเปลี่ยนแปลงระบบตามนโยบาย หรือตามมติที่ประชุมของฝ่ายต่าง ๆ

19.2.1 ฝ่ายสารสนเทศได้รับแจ้งให้มีการปรับปรุงเปลี่ยนแปลง หรือพัฒนาระบบจากมติที่ประชุมของส่วนงานต่าง ๆ

19.2.2 ฝ่ายสารสนเทศ เสนอขออนุมัติการแก้ไขโปรแกรมจากกรรมการผู้จัดการ หรือรองกรรมการผู้จัดการ

19.2.3 ฝ่ายสารสนเทศ ดำเนินการแจ้งผู้พัฒนาระบบแก้ไขโปรแกรม

19.2.4 ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบทดสอบ (Development System)

19.2.5 ฝ่ายสารสนเทศและผู้ใช้งานตรวจสอบข้อมูลในระบบทดสอบ

19.2.6 ฝ่ายสารสนเทศยืนยันความถูกต้องของโปรแกรม และแจ้งให้ผู้พัฒนาระบบนำโปรแกรมขึ้นระบบ (Production System)

19.2.7 ฝ่ายสารสนเทศติดตามประเมินผลการแก้ไขเปลี่ยนแปลงหลังจากมีการปรับปรุง

19.3 ฝ่ายสารสนเทศจัดทำทะเบียนคุมการแก้ไข พัฒนาระบบโปรแกรมปฏิบัติการ

20. กำหนดข้อตกลงระดับการให้บริการด้านเทคโนโลยีสารสนเทศทั้งภายในและภายนอกองค์กร (Service Level Agreement: SLA)

การให้บริการด้านเทคโนโลยีสารสนเทศต้องมีข้อตกลงที่ชัดเจนระหว่างผู้ใช้บริการและผู้ให้บริการ ทั้งภายนอกและภายในองค์กร เพื่อกำหนดมาตรฐาน สร้างความเข้าใจร่วมกัน และเพิ่มประสิทธิภาพการใช้งาน โดยต้องสอดคล้องกับเป้าหมายเชิงกลยุทธ์ โดยแบ่งเป็น 2 กลุ่มหลัก ดังนี้

20.1 คุณสมบัติของผู้ให้บริการสารสนเทศภายนอกองค์กร

20.1.1 ผู้ให้บริการต้องจัดทำและปฏิบัติตาม SLA อย่างชัดเจน ระบุขอบเขต ระยะเวลา และระดับความพร้อมของระบบ พร้อมแสดงความเชี่ยวชาญด้านเทคโนโลยีที่เกี่ยวข้อง

20.1.2 ต้องมีระบบบริหารจัดการความปลอดภัยของข้อมูลที่ครอบคลุม สอดคล้องกับข้อกฎหมายและเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

20.1.3 ต้องสามารถประเมินและรายงานผลการให้บริการตามตัวชี้วัด (KPI) ที่ตกลงไว้กับองค์กร

20.1.4 ต้องสามารถปรับตัวและตอบสนองต่อความต้องการขององค์กรได้อย่างเหมาะสม

20.1.5 มีความน่าเชื่อถือ โปร่งใส และมีข้อตกลงเกี่ยวกับการรักษาความลับของข้อมูล (Confidentiality Agreement) และสิทธิการเป็นเจ้าของข้อมูล (Data Ownership)

20.2 คุณสมบัติของผู้ให้บริการสารสนเทศภายในองค์กร

20.2.1 มีบุคลากรที่มีความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมกับภารกิจ

20.2.2 มีการจัดทำและปฏิบัติตามข้อตกลง SLA ภายในที่ชัดเจน ระหว่างหน่วยงานผู้ให้บริการและผู้ใช้บริการ

20.2.3 มีระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูล รวมถึงการเข้าถึง การจัดเก็บ การสำรอง และการป้องกันภัยคุกคามทางไซเบอร์

20.2.4 สนับสนุนและตอบสนองต่อความต้องการของหน่วยงานภายในอย่างมีประสิทธิภาพ

20.2.5 ส่งเสริมนวัตกรรมและการนำเทคโนโลยีสมัยใหม่มาใช้เพื่อเพิ่มประสิทธิภาพองค์กร

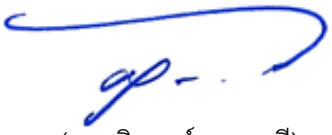
20.2.6 มีความโปร่งใส ตรวจสอบได้ และบริหารความเสี่ยงอย่างเหมาะสม

21. การทบทวนนโยบาย

ให้มีการทบทวนนโยบายการใช้งานระบบสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล และเสนอต่อคณะกรรมการบริษัทพิจารณาอนุมัติอย่างน้อยปีละ 1 ครั้ง

จึงประกาศให้ทราบและปฏิบัติโดยทั่วกันนับตั้งแต่วันที่ลงนามในท้ายประกาศ โดยนโยบายการใช้งานระบบสารสนเทศและระบบเครือข่ายสื่อสารข้อมูล ได้รับอนุมัติจากคณะกรรมการบริษัท ในการประชุมครั้งที่ 8/2568 เมื่อวันที่ 11 พฤศจิกายน 2568

ประกาศ ณ วันที่ 25 พฤศจิกายน 2568



(นายศิวพงศ์ บุญสาลี)

กรรมการผู้จัดการ

ข้อ 3. คำนิยาม

ข้อย่อย 3.1 ระบบงานสารสนเทศที่เกี่ยวข้องกับการให้บริการลูกค้า ระบบงานด้านการบริหารงานต่าง ๆ และระบบการจัดการข้อมูลสารสนเทศที่ใช้ในกิจการของบริษัทฯ ซึ่งได้แก่

1. ระบบปฏิบัติการให้สินเชื่อ
   - 1.1 ระบบงานให้บริการสินเชื่อ (LMIS)
   - 1.2 ระบบงานสินเชื่อเช่าซื้อ (HPS)
   - 1.3 ระบบที่ให้บริการสินเชื่อนอกสถานที่ (SAK Money)
   - 1.4 ระบบงานจ่ายเงินสินเชื่อให้ลูกค้า (SAK PAYMENT)

2. ระบบบัญชี
   - 2.1 ระบบงานบัญชี SAP

3. ระบบภายใน
   - 3.1 ระบบงานบัญชีเงินเดือนและข้อมูลพนักงาน
   - 3.2 ระบบไฟล์กลางของสำนักงานใหญ่
   - 3.3 ระบบจดหมายอิเล็กทรอนิกส์ (e-mail)
   - 3.4 ระบบงานจัดเก็บเอกสารชุดสัญญา (DMS)
   - 3.5 Intranet Web Site ภายในบริษัท
   - 3.6 ระบบงานการแก้ไขข้อมูล (DMT)
   - 3.7 Service ที่ใช้ในการตรวจสอบก่อนการอนุญาตในการเข้าถึงบริการต่างๆ Single Sign-On (SSO)
   - 3.8 ระบบบริหารจัดการความสัมพันธ์ลูกค้า (SAK CRM)
   - 3.9 Cloud Infrastructure

4. ระบบสำหรับลูกค้าและบุคคลทั่วไป
   - 4.1 Internet Web Site ของบริษัท
   - 4.2 แอปพลิเคชันสำหรับลูกค้าและบุคคลทั่วไป (Customer App)

ข้อ 13. การสำรองข้อมูลและการเรียกคืน (Backup and Recovery)

ข้อย่อย 13.1 ระบบสารสนเทศที่มีการเพิ่ม เปลี่ยนแปลง หรือแก้ไขข้อมูลเป็นประจำทุกวัน ให้มีการสำรองข้อมูลในระบบทุกวัน ระบบที่อยู่ในข่ายดังกล่าวได้แก่

(1) ระบบงานให้บริการสินเชื่อ (LMIS)
(2) ระบบงานบัญชี SAP
(3) ระบบไฟล์กลางของสำนักงานใหญ่
(4) ระบบจดหมายอิเล็กทรอนิกส์ (e–mail)
(5) ระบบงานจัดเก็บเอกสารชุดสัญญา (DMS)
(6) ระบบงานสินเชื่อเช่าซื้อ (HPS)
(7) ระบบงานจ่ายเงินสินเชื่อให้ลูกค้า (SAK PAYMENT)
(8) ระบบบริหารจัดการความสัมพันธ์ลูกค้า (SAK CRM)
(9) ระบบที่ให้บริการสินเชื่อนอกสถานที่ (SAK Money)
(10) แอปพลิเคชันสำหรับลูกค้าและบุคคลทั่วไป (Customer App)