บทคัดย่อ

ชื่อเรื่อง : การพัฒนาระบบบัญชีและระบบการควบคุมภายใน
สำหรับสหกรณ์ที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูล : กรณีศึกษาจังหวัดพิษณุโลก

ผู้จัดทำ : นางสาวเนื่องบุญ วรรณโก

สังกัด : กรมตรวจบัญชีสหกรณ์ กระทรวงเกษตรและสหกรณ์

ปี : 2560

ปัจจุบันความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ความต้องการในการดูแลรักษาความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้นตามไปด้วย องค์กรต่างๆ ทั้งภาครัฐและภาคเอกชนต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบ เพื่อการดูแลรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กร มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่าง ๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรงและท้าทายต่อผู้บริหารองค์กรที่รับผิดชอบในการดูแลระบบเป็นอย่างมาก การดำเนินธุรกิจของสหกรณ์ในปัจจุบันได้นำระบบคอมพิวเตอร์และระบบเครือข่ายมาใช้ในการให้บริการแก่สมาชิกและการปฏิบัติงานมากขึ้น มีการพัฒนาโปรแกรมและระบบบัญชีคอมพิวเตอร์ให้สอดคล้องกับการดำเนินธุรกิจของสหกรณ์ สหกรณ์ออมทรัพย์บางแห่งมีการเชื่อมโยงกับบริการของธนาคารพาณิชย์ สมาชิกสหกรณ์สามารถรับเงินกู้และถอนเงินฝากจากบัญชีของสมาชิกที่เปิดไว้กับสหกรณ์ผ่านเครื่อง ATM ของธนาคารพาณิชย์ โดยสหกรณ์จะเป็นผู้ส่งข้อมูลเงินฝากและวงเงินกู้ฉุกเฉินที่อนุมัติมายังธนาคารล่วงหน้า เมื่อสมาชิกถอนเงินผ่านเครื่อง ATM ระบบจะมีข้อมูลรายการถอนเงินแจ้งให้กับสหกรณ์ทราบ ปัจจัยสำคัญที่ทำให้การปฏิบัติงานมีประสิทธิภาพและประสิทธิผล มีความต่อเนื่อง คือ การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งเป็นการบริหารจัดการความเสี่ยงของระบบสารสนเทศให้สามารถรักษาความลับ ความครบถ้วนสมบูรณ์และความพร้อมใช้ กระบวนการที่เกี่ยวข้องคือการกำหนดระบบควบคุม ได้แก่ การพิสูจน์ตัวตน การกำหนดสิทธิ์ การเฝ้าตรวจความมั่นคงปลอดภัย การกำหนดนโยบายการรักษาความมั่นคงปลอดภัย โดยกระบวนการต่าง ๆ เหล่านี้หากได้กระทำอย่างถูกต้องสมบูรณ์ จะทำให้มั่นใจได้ว่าระบบสารสนเทศที่มีอยู่นั้นปฏิบัติงานได้อย่างมั่นคงปลอดภัย

จากการศึกษาเพื่อพัฒนาระบบบัญชีและระบบการควบคุมภายในสำหรับสหกรณ์ที่ใช้คอมพิวเตอร์ในการประมวลผลในจังหวัดพิษณุโลก ปัญหาที่พบคือสหกรณ์ทั้งหมดไม่มีการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษร ทำให้ผู้ใช้งานในระบบบัญชีคอมพิวเตอร์ไม่มีแนวทางในการปฏิบัติงานที่ชัดเจน ยังไม่ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ ส่งผลให้ระบบการควบคุมภายในเกี่ยวกับระบบสารสนเทศทางบัญชีของสหกรณ์มีความเสี่ยง ผู้ศึกษาจึงได้นำผลการศึกษามาจัดทำร่างนโยบายและแนวปฏิบัติในการรักษาความมั่นคง

ปลอดภัยด้านสารสนเทศของสหกรณ์ เพื่อให้สหกรณ์ใช้เป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และนำไปประยุกต์ใช้ในการกำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับการทำงานของสหกรณ์ สำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมการรักษาความลับ ความครบถ้วน และสภาพพร้อมใช้งานของระบบสารสนเทศ และสารสนเทศทางบัญชีสหกรณ์ในระบบอยู่ในระดับที่ปลอดภัย

การจัดให้มีการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้คณะกรรมการดำเนินการสหกรณ์ใช้เป็นเครื่องมือในการควบคุมการปฏิบัติงานของเจ้าหน้าที่ ผู้ตรวจสอบกิจการสหกรณ์สามารถใช้เป็นแนวทางในการปฏิบัติงานตรวจสอบด้านระบบสารสนเทศ และผู้ใช้งานในระบบสารสนเทศของสหกรณ์ตระหนักรู้และถือปฏิบัติอย่างเคร่งครัด จะช่วยให้การดำเนินการใด ๆ ของระบบเทคโนโลยีสารสนเทศของสหกรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งช่วยป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด จากผู้ใช้งานทุกฝ่ายที่ต้องทำอย่างต่อเนื่อง มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ มีการปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจึงจะเป็น“เครื่องมือ”ให้กับผู้ใช้บริการ ผู้ดูแลระบบ ผู้ใช้งานและผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสหกรณ์ทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์อย่างมีประสิทธิภาพเกิดประสิทธิผลแก่สหกรณ์

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของสหกรณ์จะสำเร็จได้ก็ต่อเมื่อบุคลากรของสหกรณ์นั้น มีการบริหารจัดการกำหนดนโยบายที่เกี่ยวข้อง มีการปฏิบัติงานและควบคุมการดำเนินการให้เป็นไปตามนโยบายที่กำหนด มีการเสริมสร้างความรู้ความเข้าใจ การพัฒนาความรู้ การสร้างการตระหนักรู้ และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม การพัฒนาระบบบัญชีและระบบการควบคุมภายในสำหรับสหกรณ์ที่ใช้คอมพิวเตอร์ในการประมวลผล จึงจะเกิดประโยชน์และสัมฤทธิผลแก่สหกรณ์อย่างแท้จริง

ข้อเสนอแนะ

จากการศึกษาในการพัฒนาระบบบัญชีและการควบคุมภายในสำหรับสหกรณ์ที่ใช้คอมพิวเตอร์ในการประมวลผล มีกรอบในการดำเนินการที่เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัย โดยให้ความสำคัญกับความเสี่ยงและผลกระทบด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น และส่งผลให้การดำเนินกิจกรรมทางธุรกิจของสหกรณ์ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ กระทบต่อการดำเนินธุรกิจของสหกรณ์ ข้อเสนอแนะการควบคุมความเสี่ยงที่เกี่ยวข้องกับระบบคอมพิวเตอร์และระบบเครือข่ายและสารสนเทศของสหกรณ์ มีดังต่อไปนี้

1. โครงสร้างและการบริหารจัดการ หากงานด้านเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ก็อาจก่อให้เกิดความเสียหายได้ การบริหารจัดการด้านโครงสร้างที่สหกรณ์ควรให้ความสำคัญ คือ การแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการกำกับดูแลและควบคุมการปฏิบัติงาน ดังนี้

1.1 การแบ่งแยกอำนาจหน้าที่ การแบ่งแยกอำนาจหน้าที่และความรับผิดชอบด้านเทคโนโลยีสารสนเทศ ควรเป็นไปตามหลักการควบคุมภายในที่ดี ไม่ควรมอบหมายให้เจ้าหน้าที่คนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ การมอบหมายให้เจ้าหน้าที่คนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบบัญชีคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย เช่น การมอบหมายเจ้าหน้าที่พัฒนาระบบงานซึ่งควรปฏิบัติงานเฉพาะในส่วนที่มีไว้สำหรับการพัฒนาระบบงาน ให้ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับส่วนของการใช้งานควบคู่กัน ความเสี่ยงในกรณีที่เจ้าหน้าที่พัฒนาระบบงาน อาจแก้ไขเปลี่ยนแปลงข้อมูลจริงหรือการทำงานของระบบบัญชีคอมพิวเตอร์ได้โดยง่าย เนื่องจากมีความรู้ความเข้าใจในการทำงานของโปรแกรมต่าง ๆ และโครงสร้างของข้อมูล เป็นต้น

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะกรรมการดำเนินการสหกรณ์และผู้ตรวจสอบกิจการควรให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างเจ้าหน้าที่ภายในหน่วยงาน โดยไม่ควรมอบหมายให้เจ้าหน้าที่คนใดคนหนึ่งรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ทั้งนี้ หากมีข้อจำกัดด้านบุคลากรโดยมีความจำเป็นต้องมอบหมายให้เจ้าหน้าที่คนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กัน ไม่สามารถแบ่งแยกหน้าที่ได้อย่างสมบูรณ์ คณะกรรมการดำเนินการสหกรณ์ควรกำหนดมาตรการหรือวิธีการกำกับดูแล และควบคุมการปฏิบัติงานของเจ้าหน้าที่รายดังกล่าวให้รอบคอบและรัดกุมเพียงพอ เช่น กำหนดให้มีบันทึกการทำงาน (log files) ในระบบงานคอมพิวเตอร์ของเจ้าหน้าที่ และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ กำหนดให้มีการหมุนเวียนสับเปลี่ยนหน้าที่และติดตามดูแลการปฏิบัติงานอย่างใกล้ชิด ไม่ควรให้เจ้าหน้าที่ที่นำข้อมูลเข้าสู่ระบบงานคอมพิวเตอร์ เป็นผู้ตรวจสอบและกระทบยอดรายงานที่ได้จากการประมวลผลข้อมูลหรือข้อมูลผลลัพธ์ หากผู้เจ้าหน้าที่มีไม่มากและขาดความรู้ความชำนาญ การแบ่งแยกหน้าที่จึงกลายเป็นเรื่องยุ่งยากในการปฏิบัติ อาจทำให้ประสิทธิภาพในการควบคุมลดน้อยลง คณะกรรมการดำเนินการสหกรณ์ควรจัดให้มีการควบคุมภายในชนิดอื่นเพื่อชดเชยประสิทธิภาพที่ลด

น้อยลง เช่น อาจมอบหมายให้กรรมการคนใดคนหนึ่งหรือหลายคนให้มีหน้าที่กำกับดูแลติดตามการปฏิบัติงานอยู่เป็นประจำ หรืออาศัยการตรวจสอบของผู้ตรวจสอบกิจการเป็นเครื่องมือที่ช่วยในการควบคุม

1.2 การกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดนโยบาย แนวปฏิบัติและขั้นตอนการปฏิบัติด้านเทคโนโลยีสารสนเทศที่ชัดเจนเป็นลายลักษณ์อักษร จะทำให้เจ้าหน้าที่สามารถปฏิบัติงานได้อย่างถูกต้อง ครบถ้วน และเป็นไปในแนวทางเดียวกัน ซึ่งจะส่งผลให้การปฏิบัติงานโดยรวมมีประสิทธิภาพนอกจากนี้ ยังลดโอกาสการปฏิบัติงานผิดพลาด ในกรณีที่มีการสับเปลี่ยนหน้าที่และความรับผิดชอบ หรือมีการมอบหมายงานให้เจ้าหน้าที่รายใหม่

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะกรรมการดำเนินการสหกรณ์/ผู้จัดการสหกรณ์ ควรให้ความสำคัญกับความครบถ้วนและความชัดเจนของการกำหนดนโยบายแนวปฏิบัติและขั้นตอนการปฏิบัติด้านเทคโนโลยีสารสนเทศ โดยเฉพาะนโยบายและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ การพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการปฏิบัติงานประจำอื่นที่สำคัญ เสริมเนื้อหาแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เข้ากับหลักสูตรฝึกอบรมต่าง ๆ ตามแผนการฝึกอบรมของสหกรณ์ เผยแพร่ประชาสัมพันธ์/รณรงค์ให้ความรู้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

1.3 การกำกับดูแลและตรวจสอบการปฏิบัติงาน การกำกับดูแลและตรวจสอบการปฏิบัติงานของเจ้าหน้าที่ระดับปฏิบัติการอย่างใกล้ชิด โดยผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย จะทำให้การปฏิบัติงานรัดกุม รอบคอบ มีความถูกต้องมากขึ้น ซึ่งจะเป็นการลดโอกาสการเกิดข้อผิดพลาดหรือข้อผิดพลาดที่เกิดขึ้นถูกตรวจพบและได้รับการแก้ไขอย่างรวดเร็ว ช่วยป้องกันการปฏิบัติงานนอกเหนืออำนาจหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย ผู้ตรวจสอบกิจการสหกรณ์ ควรให้ความสำคัญกับการรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่คณะกรรมการดำเนินการสหกรณ์กำหนดไว้ นอกจากนี้ ในกรณีที่สหกรณ์ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกไม่ว่าทั้งระบบงานหรือบางส่วน คณะกรรมการดำเนินการสหกรณ์ควรให้ความสำคัญ กับระบบการกำกับดูแลและควบคุมการปฏิบัติงานของบุคคลภายนอกเช่นกัน โดยคณะกรรมการดำเนินการสหกรณ์ควรมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของสหกรณ์ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้จัดการสหกรณ์หรือประธานคณะกรรมการดำเนินการสหกรณ์ จัดให้มีการตรวจสอบบันทึกการทำงาน (log

files) ของบุคคลภายนอก กำหนดให้บุคคลภายนอกรายงานการปฏิบัติงานภายหลังที่ปฏิบัติเสร็จเรียบร้อยแล้ว เป็นต้น

2. การรักษาความปลอดภัยฐานข้อมูลและระบบคอมพิวเตอร์ ฐานข้อมูลของระบบคอมพิวเตอร์เป็นที่จัดเก็บแฟ้มข้อมูลเป็นความลับของลูกค้าซึ่งเป็นสมาชิกของสหกรณ์ ในการดำเนินธุรกิจสหกรณ์จะมีข้อมูลของสมาชิกซึ่งเป็นข้อมูลที่ไม่ควรเปิดเผย เช่น ข้อมูลเลขบัตรประชาชน ข้อมูลทุนเรือนหุ้น ข้อมูลเงินกู้ ข้อมูลเงินรับฝาก เป็นต้น ซึ่งในปัจจุบันสหกรณ์ที่ใช้ระบบงานบัญชีคอมพิวเตอร์ได้จัดเก็บข้อมูลสำคัญตามที่กล่าวข้างต้น ไว้ในระบบคอมพิวเตอร์และในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ ดังนั้น การเข้าถึงฐานข้อมูลควรจัดให้มีระบบการรักษาความปลอดภัยและจะต้องมีการกำหนดรหัสการเข้าถึงฐานข้อมูล ในขณะเดียวกันข้อมูลในฐานข้อมูลไม่ควรมีการเข้ารหัสข้อมูล (Encryption) เพื่อประโยชน์หากในอนาคตมีการเปลี่ยนแปลงหรือพัฒนาระบบงานในเทคโนโลยีที่แตกต่างจากไปจากเดิม หากสหกรณ์ไม่มีรหัสข้อมูลจะทำให้ไม่สามารถถอดรหัสข้อมูล (Decryption) ได้ อาจทำให้การทำงานหยุดชะงักขาดความต่อเนื่อง ดังนั้น การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ จึงเป็นเรื่องที่คณะกรรมการดำเนินการสหกรณ์จะต้องให้ความสำคัญในการกำหนดนโยบายและแนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและการป้องกันความเสียหาย และการควบคุมการเข้าถึงฐานข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการป้องกันการบุกรุกระบบเครือข่าย ดังนี้

2.1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและการป้องกันความเสียหาย เนื่องจากข้อมูลส่วนใหญ่ที่เกี่ยวข้องกับการดำเนินธุรกิจของสหกรณ์ที่ ได้ถูกจัดเก็บไว้ในระบบคอมพิวเตอร์ และในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ดังนั้นการควบคุมการเข้าออกสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้เก็บฐานข้อมูล ในการประมวลผลรวมถึงการจัดทำรายงานต่าง ๆ จึงมีความสำคัญเป็นอย่างมากในการป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ นอกจากนี้การมีระบบป้องกันความเสียหายจุดที่ตั้งอุปกรณ์คอมพิวเตอร์ก็มีความสำคัญในการป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากการบุกรุกของผู้ไม่ประสงค์ดีหรือภัยพิบัติต่าง ๆ ที่อาจเกิดขึ้น

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะกรรมการดำเนินการสหกรณ์และผู้จัดการสหกรณ์ ควรให้ความสำคัญกับการควบคุมการเข้าออกสถานที่ตั้งคอมพิวเตอร์ที่รัดกุมเพียงพอ ควรจำกัดสิทธิการเข้าออกสถานที่เฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง และจัดให้มีการตรวจสอบการเข้าออกอย่างสม่ำเสมอ ให้ความสำคัญกับการจัดให้มีระบบป้องกันความเสียหายภายในสถานที่ตั้งของเครื่องคอมพิวเตอร์ จากภัยพิบัติต่างๆ เช่น ระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ ระบบไฟฟ้าสำรอง เป็นต้น

2.2 การควบคุมการเข้าถึงฐานข้อมูลและระบบงานคอมพิวเตอร์ และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security) กรณีมีการเข้าถึง ล่วงรู้หรือแก้ไขเปลี่ยนแปลงฐานข้อมูล การทำงานของระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง นั้น อาจเกิดจากบุคคลภายในของสหกรณ์เอง สาเหตุอาจมาจากการมิได้มีระบบป้องกันที่ดีพอ เช่น มิได้มีการกำหนดรหัสผ่านในการเข้าสู่ระบบงาน

คอมพิวเตอร์อย่างรัดกุม หรือกำหนดสิทธิให้แก่ผู้ใช้งานภายในเพื่อเข้าถึงข้อมูลและระบบงานคอมพิวเตอร์ที่มาก เกินความจำเป็น เป็นต้น นอกจากนี้เทคโนโลยีในปัจจุบันได้พัฒนาให้มีการเชื่อมต่อระบบเครือข่ายภายในกับ เครื่องข่ายภายนอกมากขึ้น หากสหกรณ์มิได้มีวิธีการควบคุมที่รอบคอบและรัดกุมเพียงพอ การเชื่อมต่อใน ลักษณะดังกล่าวก็อาจเป็นช่องทางให้บุคคลภายนอกสามารถเข้าถึงฐานข้อมูลและการทำงานของระบบ คอมพิวเตอร์ผ่านระบบเครือข่ายได้ รวมถึงไวรัสคอมพิวเตอร์อื่น ๆ อาจผ่านเข้ามาทางการเชื่อมต่อระบบ เครือข่ายและสร้างความเสียหายแก่ข้อมูลและระบบคอมพิวเตอร์ได้เช่นกัน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะกรรมการดำเนินการสหกรณ์และผู้จัดการสหกรณ์ ควรให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (Authentication) และการกำหนดให้มีการใส่รหัสผู้ใช้และรหัสผ่านก่อนเข้าสู่ระบบงานคอมพิวเตอร์ โดยรหัสผ่านดังกล่าวควรมีการกำหนดความยาวขั้นต่ำ ระยะเวลาของการใช้งานรหัสผ่าน จำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดและควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา นอกจากนี้ควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และสำหรับในกรณีที่มีการเชื่อมต่อระบบเครือข่ายภายในกับเครือข่ายภายนอก ต้องจัดให้มีระบบป้องกันการบุกรุกจากบุคคลภายนอก เช่น อุปกรณ์ Firewall และระบบป้องกันไวรัสคอมพิวเตอร์ เป็นต้น รวมทั้งการใช้รหัสผ่านและสิทธิของผู้ใช้งานควรมีการตรวจสอบอย่างสม่ำเสมอ ให้มีการอนุมัติการเข้าถึงฐานข้อมูลเพื่อเปลี่ยนแปลงแก้ไขข้อมูลโดยตรงจากผู้จัดการสหกรณ์หรือผู้ที่รับผิดชอบตามที่ได้รับมอบหมายของสหกรณ์อย่างเหมาะสม

3. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) โดยทั่วไประบบงานคอมพิวเตอร์ มักมีการพัฒนาแก้ไขหรือเปลียนแปลงอยู่ตลอดเวลา เนื่องจากเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนาอย่างต่อเนื่อง ด้วยเหตุนี้วิธีการจัดการและการควบคุมเกี่ยวกับการพัฒนาแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ จึงเป็นเรื่องที่คณะกรรมการดำเนินการสหกรณ์ต้องให้ความสำคัญ โดยหากไม่มีวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ระบบงานคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้อง หรืออาจไม่เป็นไปตามความต้องการของผู้ใช้งาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ควรให้ความสำคัญกับวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ โดยหากการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ควรมีการร้องขอจากผู้ใช้งานหรือผู้รับบริการ การร้องขอนั้นควรได้รับความเห็นชอบจากคณะกรรมการดำเนินการสหกรณ์ ควรจัดทำให้เป็นลายลักษณ์อักษร และควรกำหนดให้มีการทดสอบก่อนการใช้งานจริงทั้งจากเจ้าหน้าที่พัฒนาระบบและผู้ใช้งาน เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาแก้ไขหรือเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งานและผู้ที่มีส่วนเกี่ยวข้อง นอกจากนี้ควรจัดให้มีเอกสารประกอบการพัฒนา แก้ไขหรือเปลี่ยนแปลงโปรแกรมของระบบงานคอมพิวเตอร์ ที่มีรายละเอียดเพียงพอเกี่ยวกับโปรแกรมที่ใช้อยู่ปัจจุบัน ทั้งนี้ การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามระเบียบ

ของสหกรณ์ ดังนั้นจึงควรมีการสอบทานระเบียบและกฎเกณฑ์ที่เกี่ยวข้องก่อนการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์

4. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน สิ่งที่สำคัญที่สุดในระบบสารสนเทศทางการบัญชีสหกรณ์ คือ ข้อมูลที่อยู่ในโปรแกรมระบบงานหรือระบบบัญชี เพราะสหกรณ์ลงทุนเพื่อให้ได้มาซึ่งข้อมูลสารสนเทศที่มีความถูกต้องครบถ้วน สะดวก รวดเร็ว น่าเชื่อถือ สามารถสนับสนุนการตัดสินใจหรือเป็นข้อมูลในการบริหารงานให้บรรลุวัตถุประสงค์ได้ บ่อยครั้งที่พบว่าเกิดความเสียหายที่มาจากสื่อบันทึกข้อมูลของสหกรณ์ ดังนั้นจึงจำเป็นที่ต้องจัดให้มีผู้รับผิดชอบในการจัดการสื่อบันทึกข้อมูลโดยเฉพาะ โดยรับผิดชอบดูแลรักษาสื่อบันทึกข้อมูลต่าง ๆ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card หรือ External Harddisk เป็นต้น ให้มีสภาพที่ครบถ้วนสมบูรณ์พร้อมใช้งานมีความปลอดภัย ข้อมูลที่จัดเก็บในสื่อมีความครบถ้วนถูกต้องเชื่อถือได้ มีการปรับปรุงให้เป็นปัจจุบันและมีการควบคุมการเลิกใช้งานอย่างเหมาะสม ในการดำเนินธุรกิจมีหลายกรณีที่อาจทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย เช่น การติดไวรัส การบุกรุกของผู้ไม่ประสงค์ดีหรือภัยพิบัติต่าง ๆ หรืออาจเกิดจากการปฏิบัติงานที่ผิดพลาดของผู้ใช้งาน เป็นต้น คณะกรรมการดำเนินการสหกรณ์ควรให้ความสำคัญกับการสำรองข้อมูลและระบบบัญชีคอมพิวเตอร์ รวมทั้งการเตรียมพร้อมกรณีฉุกเฉินต่าง ๆ ดังนี้

4.1 การสำรองข้อมูลและระบบบัญชีคอมพิวเตอร์ หากมิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ที่เพียงพอ ในกรณีที่เกิดเหตุการณ์ที่ทำให้ข้อมูลหรือระบบบัญชีคอมพิวเตอร์เสียหาย สหกรณ์ก็อาจไม่มีข้อมูลหรือระบบบัญชีคอมพิวเตอร์ที่มีประสิทธิภาพและในเวลาที่ต้องการ เพื่อการใช้งานได้อย่างต่อเนื่อง ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของสหกรณ์และอาจก่อให้เกิดความเสียหายต่อสมาชิกได้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ควรให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์ และมีแผนการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

4.2 การเตรียมพร้อมกรณีฉุกเฉิน การสำรองข้อมูลและระบบงานคอมพิวเตอร์เพียงอย่างเดียวอาจไม่เพียงพอแก่การป้องกันการหยุดชะงักของการดำเนินธุรกิจ ดังนั้นการจัดให้มีแผนฉุกเฉินเพื่อรองรับในกรณีที่อาจเกิดเหตุการณ์ฉุกเฉิน จะทำให้การควบคุมการดำเนินการมีประสิทธิภาพมากขึ้น

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ควรให้ความสำคัญกับการจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินต่าง ๆ ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งควรมีการทดสอบแผนดังกล่าวเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

5. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ การปฏิบัติงานประจำด้านระบบงานคอมพิวเตอร์ที่สำคัญ คือ การควบคุมการประมวลผลข้อมูล ซึ่งการประมวลผลข้อมูลที่ถูกต้องและครบถ้วนมีความสำคัญต่อการประกอบธุรกิจของสหกรณ์ ซึ่งหากมิได้มีวิธีการปฏิบัติและการควบคุมที่รอบคอบและรัดกุม

เพียงพอ อาจทำให้ข้อมูลไม่ถูกต้องหรือไม่ครบถ้วนก่อให้เกิดความเสียหายต่อสหกรณ์และสมาชิกได้ นอกจากนี้ และงานอื่นที่สำคัญ เช่น การดูแลรักษาการทำงานของระบบคอมพิวเตอร์ การโอนย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริง การสำรองข้อมูลและระบบงานคอมพิวเตอร์เดิมเก็บไว้ ซึ่งหากมิได้มีวิธีการปฏิบัติและควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจก่อให้เกิดความเสียหายด้านเทคโนโลยีสารสนเทศของสหกรณ์ได้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการดำเนินการสหกรณ์ ผู้ตรวจสอบกิจการ ควรให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างใกล้ชิด จัดให้มีการปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงานและการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

ประกาศสหกรณ์.....–ร่าง–.....

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.....

ตามระเบียบนายทะเบียนสหกรณ์ว่าด้วย “มาตรฐานขั้นต่ำในการควบคุมภายในและการรักษาความปลอดภัยสำหรับสหกรณ์และกลุ่มเกษตรกรที่ใช้โปรแกรมระบบบัญชีคอมพิวเตอร์ประมวลผลข้อมูล พ.ศ. 2553” กำหนดให้สหกรณ์ต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ของระบบเทคโนโลยีสารสนเทศของสหกรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สหกรณ์ *ชื่อสหกรณ์* จึงได้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อใช้เป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของสหกรณ์ถือปฏิบัติโดยเคร่งครัด อาศัยอำนาจตามข้อบังคับสหกรณ์ *ชื่อสหกรณ์* ข้อ *(กำหนดอำนาจหน้าที่ของกรรมการดำเนินการแต่ละตำแหน่ง)* และ ข้อ *(กำหนดอำนาจหน้าที่ของกรรมการดำเนินการ)* จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า ประกาศสหกรณ์ *ชื่อสหกรณ์* เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.....

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดแล้วก่อนหน้านี้ ซึ่งขัดหรือแย้งกับประกาศฉบับนี้ให้ใช้ประกาศฉบับนี้แทน

ข้อ 4 การจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์มีวัตถุประสงค์ ดังนี้

(1) ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสหกรณ์

(2) มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

(3) เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

(4) เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของสหกรณ์เองและขององค์กรอื่นที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

(5) เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

ข้อ 5 รายละเอียดของนโยบาย

(1) กำหนดผู้รับผิดชอบ มีการกำหนดผู้รับผิดชอบที่ชัดเจน ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สหกรณ์หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(2) กำหนดนโยบายควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน ผู้ใช้บริการหรือประชาชนทั่วไปอย่างทั่วถึง โดยให้ผู้ใช้งาน สมาชิกและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(3) กำหนดนโยบายระบบสารสนเทศและระบบสำรองสารสนเทศ มีการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน มีการแยกประเภทและการจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(4) กำหนดนโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีการตรวจสอบและประเมินความเสี่ยงรวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อการเปลี่ยนแปลงเพิ่มเติมในส่วนที่มีผลกระทบในเนื้อหารายละเอียดสำคัญ

(5) กำหนดนโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ 6 ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

(1) มีการจัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน และการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจของสหกรณ์

(3) กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

(4) มีการกำหนดการใช้งานตามภารกิจและหน้าที่เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

ข้อ 7 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ที่ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(1) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(2) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(3) การบริหารจัดการสิทธิผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ 8 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหาอย่างน้อย ดังนี้

(1) การใช้งานรหัสผ่าน (Password User) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(2) การป้องกันอุปกรณ์คอมพิวเตอร์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของสหกรณ์ในขณะที่ไม่มีผู้ดูแล

(3) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่ได้ใช้งาน

(4) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ

ข้อ 9 การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกสหกรณ์ (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกสหกรณ์สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสหกรณ์ได้

(3) การระบุอุปกรณ์บนเครือข่าย ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่าย และควรใช้อุปกรณ์บนเครือข่ายเป็นการยืนยัน

(4) การป้องกันพอร์ตที่ใช้งานสำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้งานสำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(5) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือการใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมเข้าถึง

(7) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

ข้อ 10 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(1) กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบการปฏิบัติการที่จะต้องควบคุมโดยวิธีการพิสูจน์ยืนยันตัวตน

(2) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(4) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ (Utilities) เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(5) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(6) การจำกัดระยะเวลาการเข้าถึงการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ 11 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุมอย่างน้อย ดังนี้

(1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน และผู้ที่นำข้อมูลเข้าระบบในการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน (Application) ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(2) ระบบซึ่งไวตอบการรบกวน มีผลกระทบและมีความสำคัญต่อสหกรณ์ ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีความควบคุมสภาพแวดล้อมของตนเอง

(3) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสม เพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(4) การเข้าถึง จากภายนอกสถานที่ตั้งของสหกรณ์ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติที่เหมาะสม เพื่อปรับใช้สำหรับการปฏิบัติงานของสหกรณ์ภายนอก

ข้อ 12 จัดทำระบบสำรองสำหรับระบบสารสนเทศตามแนวทางต่อไปนี้

(1) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(2) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์เพื่อให้สามารถทำงานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการปฏิบัติงานตามภารกิจ

(3) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

(4) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

(5) มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง อย่างน้อยปีละ 1 ครั้ง

ข้อ 13 มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยมีเนื้อหา ดังต่อไปนี้

(1) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit Assessment) อย่างน้อยปีละ 1 ครั้ง

(2) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบกิจการหรือสหกรณ์ภายนอก เพื่อให้สหกรณ์ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ 14 ต้องกำหนดความรับผิดชอบที่ชัดเจนกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สหกรณ์ หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงที่มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของสหกรณ์เป็นผู้รับผิดชอบต่อความเสี่ยงและเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ 15 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

ให้คณะกรรมการดำเนินการของสหกรณ์เป็นผู้รักษาการตามประกาศนี้และอำนาจวินิจฉัยตีความในกรณีที่เกิดปัญหาจากการปฏิบัติตามประกาศนี้

ประกาศ ณ วันที่.....

(.....)

ประธานกรรมการสหกรณ์.....

เอกสารแนบท้ายประกาศ

แนวนโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของ สหกรณ์.....

พ.ศ.....

สารบัญ

หน้า

หน้า

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์

หลักการและเหตุผล

ตามประกาศคณะกรรมการดำเนินการสหกรณ์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ *ชื่อสหกรณ์* พ.ศ..... กำหนดไว้ว่าต้องจัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ มีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งช่วยลดโอกาสที่จะเกิดความเสียหายต่อการดำเนินงาน ทรัพย์สินและบุคลากรของสหกรณ์ ดังนั้นสหกรณ์ *ชื่อสหกรณ์* จึงได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ฉบับนี้ขึ้น เพื่อใช้เป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ ซึ่งบุคลากรของสหกรณ์และหน่วยงานภายนอกที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด ทั้งนี้ ได้กำหนดมาตรการ แนวทางและขั้นตอนการปฏิบัติ ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ในเรื่องต่าง ๆ ตามความจำเป็น ซึ่งประกอบด้วยส่วนต่าง ๆ ดังต่อไปนี้

วัตถุประสงค์

(๑) เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ *ชื่อสหกรณ์*

(๒) เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ *ชื่อสหกรณ์* ซึ่งสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ให้แก่เจ้าหน้าที่ทุกระดับของสหกรณ์ และบุคคลที่เกี่ยวข้อง ถือปฏิบัติอย่างเคร่งครัด

(๓) เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้แก่เจ้าหน้าที่ทุกระดับของสหกรณ์ *ชื่อสหกรณ์* และบุคคลที่เกี่ยวข้อง

(๔) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

รายละเอียดของแนวปฏิบัติ

- แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ
- แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย
- แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ
- แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
- แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ
- แนวปฏิบัติในการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- แนวปฏิบัติในการใช้งานอินเทอร์เน็ต
- แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ
- แนวปฏิบัติในการการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานของสหกรณ์
- แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

คำนิยาม

คำนิยามที่ใช้ ประกอบด้วย

(1) สหกรณ์ หมายความว่า สหกรณ์ ...*ชื่อสหกรณ์*

(2) ผู้บริหารระดับสูง หมายถึง ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่บริหารจัดการและดูแลระบบสารสนเทศของสหกรณ์

(3) ผู้ใช้งาน หมายความว่า เจ้าหน้าที่/พนักงาน ลูกจ้างและบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานเครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ตของสหกรณ์

(4) ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ของสหกรณ์ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบสารสนเทศ หรือระบบเครือข่าย หรือระบบคอมพิวเตอร์ของสหกรณ์

(5) เจ้าหน้าที่ หมายความว่า เจ้าหน้าที่/พนักงาน ลูกจ้าง ผู้ดูแลระบบและผู้บริหารของสหกรณ์ ผู้รับบริการ ผู้ใช้งานทั่วไป

(6) สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับ ระบบสารสนเทศของสหกรณ์

(7) ทรัพย์สิน หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับสหกรณ์

(8) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(9) ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(10) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการ ป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(11) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสหกรณ์ถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

(12) ระบบเครือข่าย หมายความว่า กลุ่มของคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และสื่อนำสัญญาณที่ถูกนำมาเชื่อมต่อกันผ่านอุปกรณ์ด้านการสื่อสารหรือสื่ออื่นใด ซึ่งคณะกรรมการดำเนินการสหกรณ์หรือผู้ที่ได้รับมอบหมาย เป็นผู้กำหนดและทำให้ผู้ใช้ในระบบเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนและใช้อุปกรณ์หรือทรัพยากรต่าง ๆ ของเครือข่ายร่วมกันได้ โดยเครือข่ายคอมพิวเตอร์จะครอบคลุมทั้งเครือข่ายภายในหรือแลน (Local Area Network : LAN) เครือข่ายไร้สายหรือไวเลสแลน (Wireless LAN : WLAN) และเครือข่ายวงกว้างหรือแวน (Wide Area Network : WAN) ของสหกรณ์

(13) ระบบสารสนเทศ หมายความว่า ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ Hardware, Software, User/People, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกัน เพื่อกำหนดรวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูล เพื่อสร้างสารสนเทศและส่งผลลัพธ์หรือสารสนเทศที่ได้ให้กับผู้ใช้งาน เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และติดตามผลการดำเนินงานของสหกรณ์

(14) ระบบงานของสหกรณ์ หมายความว่า ระบบสารสนเทศที่ใช้ในการดำเนินธุรกรรมและการดำเนินงานของสหกรณ์

(15) การใช้งานอินเทอร์เน็ต หมายความว่า การใช้บริการต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ตของสหกรณ์

(16) คอมพิวเตอร์ หมายความว่า อุปกรณ์คอมพิวเตอร์ที่มีการเชื่อมต่อเพื่อใช้งานเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตที่สำนักงานสหกรณ์

(17) ข้อมูล หมายความว่า สิ่งที่ป้อนเข้าไปในคอมพิวเตอร์ ไม่ว่าจะเป็นตัวเลข ข้อความ คำสั่ง ชุดคำสั่ง ซอฟต์แวร์ แฟ้มข้อมูล หรือรายละเอียดซึ่งอาจอยู่ในรูปแบบประเภทต่างๆ

(18) รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(19) จดหมายอิเล็กทรอนิกส์ (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

(20) ชุดคำสั่งไม่พึงประสงค์ดี (Malware) หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(21) หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานที่สหกรณ์อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสหกรณ์ โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล หรือหน่วยงานที่สหกรณ์ดำเนินการส่งหรือเข้าถึงข้อมูลสารสนเทศ

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

1. ต้องแบ่งแยกเจ้าหน้าที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากเจ้าหน้าที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)

2. ต้องจัดให้มีการจัดทำรายละเอียดหน้าที่และความรับผิดชอบ (Job Description) ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของเจ้าหน้าที่แต่ละคนภายในฝ่ายคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

3. ควรจัดให้มีเจ้าหน้าที่สำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้ดูแลระบบ เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ เป็นต้น

บทบาทและความรับผิดชอบ

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ ต่อสหกรณ์หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์และป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและ ความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

1. ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์

2. ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ โดยกำหนดมาตรการและกำกับดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์แนบท้ายประกาศนี้

3. ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์

4. ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์

หน้าที่ความรับผิดชอบของผู้ดูแลระบบ

1. จัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

2. บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของสหกรณ์ เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้หรือสูญหาย

3. เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่ายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

4. กำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ตามที่ได้รับมอบหมาย โดยกำหนดสิทธิ์ให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

5. บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นต้องป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อสหกรณ์ ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

6. ติดตั้งและเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ที่ได้รับมอบหมาย และทบทวนการกำหนดค่าพารามิเตอร์ต่าง ๆ อย่างน้อยเดือนละครั้ง

7. บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของสหกรณ์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงให้มีความปลอดภัย

8. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของ สหกรณ์ เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

9. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

10. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

11. คืนทรัพย์สินของสหกรณ์ ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้คณะกรรมการดำเนินการสหกรณ์หรือผู้ที่ได้รับมอบหมายทำการตรวจสอบการคืนทรัพย์สิน

หน้าที่ความรับผิดชอบของผู้ใช้งาน

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบ ทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติดังนี้

1. การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(1) ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(2) ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

(3) ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(4) ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(5) ผู้ใช้งานควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

(6) ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

(7) ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(8) ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 1234, ABCD หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น 99999 , aaaaa เป็นต้น

(9) ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด หรืออย่างน้อยทุกๆ ๖ เดือน

(10) ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(11) ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการบันทึกเข้าสู่ระบบงาน

(12) ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้เพื่อความสะดวกของตนเองเมื่อทำการเข้าสู่ระบบงาน (Login) ในภายหลัง

(13) ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

(14) ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

2. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(1) ผู้ใช้งานควรออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ โดยทันทีเมื่อเสร็จสิ้นงาน เช่น ออกจากระบบงานแล้วปิดเครื่องคอมพิวเตอร์หรือเครื่องโน้ตบุ๊กที่ใช้งาน

(2) ผู้ใช้งานควรล็อค (Lock) อุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(3) ผู้ใช้งานควรป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(4) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อค (Lock) หน้าจอ หลังจากที่ไม่ได้ใช้งานมาช่วงระยะเวลาหนึ่ง เช่น 15 นาที หลังจากที่มีการล็อค (Lock) หน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(5) ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้เจ้าหน้าที่เข้าใจในมาตรการป้องกันที่ได้กำหนดไว้นั้น

(6) ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้นหรือไม่มีการใช้งานนานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ซึ่งต้องใช้งานตลอด 24 ชั่วโมง

3. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์การควบคุมทรัพย์สินสารสนเทศ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลและแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศ และข้อมูลสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์โดยมีแนวทางปฏิบัติ ดังนี้

(1) ผู้ใช้งานต้องป้องกันทรัพย์สินของสหกรณ์ และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยโดยให้ครอบคลุมเรื่องต่าง ๆ ประกอบด้วย

- การจัดการบริเวณโดยรอบ
- การควบคุมการเข้า - ออกพื้นที่
- การจัดการบริเวณของการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การจัดวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

(3) ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของสหกรณ์ก่อนเข้าใช้งานโดยใช้กลไกการพิสูจน์ยืนยันตัวตนที่เหมาะสม

(4) ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของสหกรณ์
- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับหรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน

- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องถ่ายเอกสาร เครื่องสแกนเอกสาร เป็นต้น

- นำเอกสารสำคัญหรือเอกสารลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึก คอมพิวเตอร์ หรือสารสนเทศออกจากสหกรณ์ ต้องขออนุมัติจากผู้จัดการสหกรณ์หรือผู้ที่รับการมอบหมายก่อนทุกครั้ง

(6) ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(7) ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของสหกรณ์ เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้หรือสูญหาย

(8) ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(9) การทำลายข้อมูลอิเล็กทรอนิกส์ มีวิธีการ ดังนี้

เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้ที่ได้รับมอบหมายให้ทำลายข้อมูลจะต้องเป็นผู้ดำเนินการ โดยมีวิธีการดำเนินการดังต่อไปนี้

ประเภท สื่อบันทึกข้อมูล	**วิธีการทำลาย**
Flash Drive, Memory Card	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกาDOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

การเข้าถึงและควบคุมการใช้งานระบบคอมพิวเตอร์หรือสารสนเทศ

ต้องจัดทำนโยบายและแนวปฏิบัติ ในการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษรและปรับปรุงอย่างน้อยปีละ 1 ครั้ง โดยการจัดทำนโยบายนี้ จะพิจารณาจากความต้องการทางการปฏิบัติงาน และทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ซึ่งมีแนวทางปฏิบัติ ดังนี้

(1) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

- ต้องจัดทำนโยบายการใช้งานบริการเครือข่าย (Policy on Use of Network Services) ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้งานได้ บริการใดไม่สามารถใช้งานได้
- ต้องมีการพิสูจน์ยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกสหกรณ์ (User Authentication for External Connections) ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของสหกรณ์ได้
- ต้องมีการพิสูจน์ยืนยันตัวตนอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้สามารถระบุและพิสูจน์ตัวตน เพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว
- ต้องมีการแบ่งแยกเครือข่าย (Segregation in Networks) ตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- ต้องมีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายในการควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางการปฏิบัติงานได้ระบุไว้
- ต้องมีการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบาย ในการควบคุมการเข้าถึง

(2) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

- ต้องมีการปฏิบัติตามขั้นตอนในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on Procedures) สำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ
- ต้องมีการระบุและพิสูจน์ยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกันและต้องจัดให้มีกระบวน การพิสูจน์ยืนยันตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ
- ต้องจัดให้มีระบบบริหารจัดการรหัสผ่าน (Password Management System) ที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ
- ต้องมีการจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (User of System Utilities) เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

- ต้องกำหนดให้มีการหมดเวลาการใช้งานระบบสารสนเทศ (Session Time - Out) โดยกำหนดให้ระบบตัดการใช้งานของผู้ใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง
- ต้องมีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ของระบบสารสนเทศที่มีความสำคัญสูง

(3) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and information Access Control)

- ต้องมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชั่นต่าง ๆ ของแอพพลิเคชั่น (Information Access Restriction) โดยการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน
- ต้องมีการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) ไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

4. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยมีแนวปฏิบัติ ดังนี้

(1) ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน

(2) กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

(3) ต้องมีการเชื่อมต่อโดยการเข้ารหัส ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ Web Application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์

(4) จำนวนช่องทางที่เหมาะสมกับสหกรณ์ ที่สามารถเข้าถึงได้ดังต่อไปนี้

- ติดต่อด้วยตนเอง เข้าถึงได้ในเวลาราชการ
- ระบบโทรศัพท์เข้าถึงได้ในเวลาราชการ
- หนังสือหรือบันทึกข้อความเข้าถึงได้ทุกช่วงเวลา)
- ระบบเครือข่ายภายใน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนดเวลา)
- การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และช่วงเวลาพิเศษเป็นรายครั้ง)

(5) กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

- วิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล
- วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย

- บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย

(6) ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้

- ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่สหกรณ์กำหนด
- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

(7) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของสหกรณ์ เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

(8) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเก็บไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติและมีการปรับปรุงข้อมูลให้เป็นปัจจุบันหรือไม่

(9) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ (Update Version/Update Program) ในเครื่องตามปกติหรือไม่

(10) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย มีแนวทางปฏิบัติ ดังนี้

1. ผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย ทำหน้าที่กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและระบบข้อมูล เพื่อจุดประสงค์ในการเฝ้าระวัง การควบคุม การรักษา ความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจจะเกิดขึ้นได้

2. การกำหนดและจำแนกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ประกอบด้วย พื้นที่ส่วนต่าง ๆ ตามตำแหน่งของพื้นที่ใช้งาน แบ่งออกเป็นพื้นที่ทำงานทั่วไปของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและผู้ดูแลระบบ พื้นที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และจัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ติดตั้งอุปกรณ์ระบบเครือข่าย (Network Equipment area) พื้นที่ห้องควบคุมระบบไฟฟ้าสำรอง

3. การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์เข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายและทำการปรับปรุงรายการผู้มีสิทธิ์เข้า - ออกพื้นที่ทุกครั้งที่มีการเปลี่ยนแปลง

การควบคุมการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์

การควบคุมการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ มีแนวทางปฏิบัติ ดังนี้

1. ผู้ดูแลระบบจัดทำเอกสารแบบฟอร์มการบันทึกการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สหกรณ์ ซึ่งต้องระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน พื้นที่หรือเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ์ รายละเอียดกิจกรรม ระยะเวลาดำเนินการ และบันทึกการเข้า - ออกพื้นที่ใช้งานอย่างสม่ำเสมอ

2. ผู้ดูแลระบบตรวจสอบการบันทึกการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สหกรณ์ทุกครั้งที่มีการใช้งาน และบันทึกรายการอุปกรณ์ให้ถูกต้อง โดยผู้ดูแลระบบจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา รวมทั้ง ตรวจสอบการบันทึกการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์เป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

3. ผู้ดูแลระบบควรมีระบบป้องกันและตรวจสอบการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์อย่างปลอดภัย เช่น ติดบัตรแสดงตนว่าเป็นผู้ได้รับสิทธิ หรือสมาร์ทการ์ด (Smart card) เป็นต้น

4. ผู้ใช้งานที่ต้องการเข้าใช้ห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สหกรณ์ จะต้องขออนุญาตและบันทึกการเข้า - ออกพื้นที่ทุกครั้ง

5. หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้งาน ขอเข้าใช้ห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์ โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ผู้ดูแลระบบต้องตรวจสอบเหตุผลและความจำเป็น ก่อนอนุญาตและจดบันทึกการเข้า - ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

ผู้ดูแลระบบห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์

ผู้ดูแลระบบห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ มีแนวทางปฏิบัติ ดังนี้

1. สิทธิ์ในการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ของเจ้าหน้าที่แต่ละคนต้องได้รับ การอนุมัติจากผู้จัดการสหกรณ์หรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์ และจัดให้มีการทบทวนสิทธิอย่างน้อยปีละ 1 ครั้ง

2. การเข้าถึงห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์ ต้องมีการลงบันทึกไว้ในเอกสารแบบฟอร์มการเข้า - ออกทุกครั้ง

3. ต้องจัดทำระบบการจัดเก็บบันทึกการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สหกรณ์ไว้ด้วย

4. กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์ ผู้ดูแลระบบจะต้องควบคุมอย่างรัดกุม

ผู้ติดต่อจากหน่วยงานภายนอก

มีแนวทางปฏิบัติ ดังนี้

1. ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผู้ติดต่อ ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสหกรณ์

2. ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาปฏิบัติงานในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ ตามที่ระบุไว้ในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ให้ถูกต้องชัดเจน

3. ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับผู้ดูแลระบบ ซึ่งผู้ดูแลระบบต้องตรวจสอบการคืนบัตร และตรวจสอบการลงบันทึกตามเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์ทุกครั้ง

4. ผู้ดูแลระบบควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสหกรณ์เป็นประจำทุกเดือน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

1. แนวกำหนดเครือข่ายไร้สายนี้ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสหกรณ์ และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง Wireless Policy อาจมีการเปลี่ยนแปลงตามเทคโนโลยีใหม่ และกระบวนการที่สอดคล้องและเหมาะสม

2. ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าการให้บริการ และการเชื่อมต่อเครื่องไร้สายทั้งหมด

3. การจัดการจุดเชื่อมต่อไร้สายในพื้นที่สหกรณ์ จะต้องถูกตรวจสอบอุปกรณ์ติดตั้ง และกำหนดค่าโดยผู้ดูแลระบบเท่านั้น

4. ทุกจุดเชื่อมต่อเครือข่ายไร้สายและอุปกรณ์ที่เกี่ยวข้อง เช่น Access Point จุดเชื่อมต่อสายสัญญาณ Switch จะต้องมีความปลอดภัย มีรูปแบบในการจัดเก็บและเข้าถึงอุปกรณ์

5. ฟังก์ชันที่ใช้ในการตั้งค่าของจุดเชื่อมต่อจะต้องสามารถเข้าถึงได้เฉพาะผู้ที่มีหน้าที่ในการดูแลระบบ

6. จุดเชื่อมต่อจะต้องมีการกำหนดค่า Gateway ที่เป็นค่าที่กำหนดไว้ของเครือข่ายเฉพาะส่วนเท่านั้น

7. ผู้ดูแลระบบต้องเปลี่ยนชื่อเครือข่ายไร้สาย (ค่า SSID : Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

8. ชื่อเครือข่ายไร้สายที่กำหนด จะต้องถูกต้องตามรูปแบบ และจะต้องไม่มีการบ่งบอก หรือแสดงตำแหน่งของสายที่จุดเชื่อม LAN หรือ ชื่ออื่นๆ

9. ชื่อเครือข่ายไร้สายจะต้องถูกยกเลิกค่าการส่งสัญญาณกระจายในเครือข่าย (Broadcast) ยกเว้นจุดที่ได้รับอนุญาต

10. อุปกรณ์ต่าง ๆ จะไม่สามารถเชื่อมต่อกับเครือข่ายไร้สายได้ จนกว่าจะสามารถระบุชื่อเครือข่ายไร้สายที่ถูกต้อง ในกรณีที่มีการยกเลิกค่าการ Broadcast

11. เลือกใช้เทคโนโลยี Authentication และมีการกำหนดค่าการเข้ารหัสในการเชื่อมต่อ

12. อุปกรณ์ที่ใช้ในการเข้าถึงเครือข่ายของสหกรณ์ จะต้องรองรับมาตรฐานที่เหมาะสมกับสถานะการณ์ปัจจุบันของสหกรณ์ การเชื่อมต่อจะต้องมีซอฟต์แวร์ป้องกันไวรัส

13. ทุกจุดเชื่อมจะต้องกำหนดรหัสผ่านเพื่อเข้าใช้งาน คุณลักษณะการจัดการรหัสผ่านนี้จะถูกเก็บไว้และส่งในรูปแบบที่เข้ารหัส

14. อุปกรณ์เครือข่ายไร้สายทั้งหมดต้องได้รับความเห็นชอบจากคณะกรรมการดำเนินการสหกรณ์

15. ห้ามไม่ให้เจ้าหน้าที่หรือทีมงานเครือข่ายบอกค่าติดตั้งของเครือข่ายไร้สายกับผู้ใช้งานหรือบุคคลภายนอก

16. ผู้ดูแลระบบมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายไร้สายของอุปกรณ์ทุกชนิด ที่ไม่เป็นไปตามนโยบายหรือมีความเสี่ยงต่อระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

17. ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

1. ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมด

2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกปิดกั้นโดยไฟร์วอลล์

4. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

5. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

6. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อ พื้นฐานของโปรแกรมทั่วไป ที่ทางสหกรณ์อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือ ที่กำหนดจะต้องได้รับความยินยอมจากสหกรณ์

7. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่า อนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่าย เป็นรายเครื่องที่ให้บริการจริง

8. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

9. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

10. สหกรณ์มีสิทธิ์ที่จะระงับหรือปิดกั้นการใช้งานของคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

11. การเชื่อมต่อในลักษณะของการเข้าใช้ระบบคอมพิวเตอร์ระยะไกล (Remote Login) จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในของสหกรณ์ จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมาย

12. ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

การรักษาความมั่นคงปลอดภัยของระบบตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy)

1. การรักษาความมั่นคงปลอดภัยของระบบตรวจจับการบุกรุก (IDS/IPS Policy) เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศและข้อมูลบนเครือข่ายภายในสหกรณ์ ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

2. การรักษาความมั่นคงปลอดภัยของระบบตรวจจับการบุกรุก (IDS/IPS Policy) ครอบคลุมทุกโฮสต์ในเครือข่ายของสหกรณ์ และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

3. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบตรวจจับการบุกรุก

4. ระบบทั้งหมดในเขตปลอดภัย (De Militarized Zone : DMZ) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

5. โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านระบบตรวจจับการบุกรุก (IDS/IPS) จะต้องมีการบันทึกผลการตรวจสอบ

6. มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งาน เครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

7. ระบบตรวจจับการบุกรุก (IDS/IPS) จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

8. เครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้งแบบ Host - Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

9. พฤติกรรมการใช้งาน กิจกรรมหรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ประธานคณะกรรมการดำเนินการสหกรณ์ทราบทันทีที่ตรวจพบ

11. พฤติกรรมกิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบ จะต้องมีการรายงานให้ประธานคณะกรรมการดำเนินการสหกรณ์ทราบภายใน 1 ชั่วโมงที่ตรวจพบ

12. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน

13. ผู้ดูแลระบบมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้ล่วงหน้า

14. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของสหกรณ์ การพยายามเข้าถึง ระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของสหกรณ์จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

1. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

2. กำหนดให้มีการบันทึกให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึกการเข้า-ออกระบบบันทึก การพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง

3. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

การป้องกันไวรัสและภัยคุกคามอื่น ๆ ในการใช้งานคอมพิวเตอร์

1. ผู้ใช้งานควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ในสื่อบันทึกข้อมูล เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card หรือ External Harddisk หรือ Could เป็นต้น เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

2. ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัสที่ได้ติดตั้งไว้

3. ผู้ใช้งานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการปรับปรุงซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ผู้มีหน้าที่รับผิดชอบทราบหากไม่สามารถปรับปรุงซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

4. ผู้ใช้งานต้องแจ้งให้มีหน้าที่รับผิดชอบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

5. ผู้ใช้งานต้องตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นทุกครั้ง เมื่อมีการติดตั้งหรือใช้งานด้วยซอฟต์แวร์ป้องกันไวรัส และหากตรวจพบไวรัสจะต้องรีบจัดการทำลายไวรัสโดยเร็วที่สุด หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมนั้น ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องที่ใช้งานอยู่เด็ดขาด

การใช้เครื่องคอมพิวเตอร์อย่างปลอดภัยและมีประสิทธิภาพ

1. ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์คอมพิวเตอร์ใด ๆ ลงบนเครื่องคอมพิวเตอร์ หากมีความจำเป็นในการติดตั้งซอฟต์แวร์จะต้องแจ้งให้ผู้ดูแลระบบทราบ

2. ห้ามผู้ใช้งานติดตั้งอุปกรณ์เครือข่ายเพิ่มเติม เว้นแต่จะให้ผู้ดูแลระบบดำเนินการให้

3. ผู้ใช้งานที่ต้องการนำคอมพิวเตอร์มาใช้งานภายใต้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตที่สหกรณ์จัดสรรให้ จะต้องมีซอฟต์แวร์ป้องกันไวรัสซึ่งสามารถปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และต้องสามารถตรวจจับโปรแกรมไม่ประสงค์ดี (Malware) อื่น ๆ เช่น Spyware ได้ด้วยหรือแจ้งผู้ดูแลระบบให้ทำการติดตั้งซอฟต์แวร์ป้องกันไวรัสให้

4. ห้ามผู้ใช้งานใช้โปรแกรมประเภทดักจับข้อมูลผู้ใช้งานบนเครือข่าย

การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

1. เสริมเนื้อหาแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เข้ากับหลักสูตรฝึกอบรมต่าง ๆ ตามแผนการฝึกอบรมของสหกรณ์

2. เผยแพร่ประชาสัมพันธ์/รณรงค์ให้ความรู้ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้หรือข้อระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) มีวิธีการปฏิบัติ ดังนี้

การลงทะเบียนผู้ใช้งาน (User Registration)

1. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ โดยต้องระบุข้อมูลพื้นฐานเป็นอย่างน้อย ดังนี้ ชื่อและนามสกุล ตำแหน่ง หน่วยงาน

2. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งานว่าไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

3. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

4. ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

5. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์โดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

6. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์โดยไม่ได้รับอนุญาต

การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2. ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสม สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์

3. ผู้ดูแลระบบต้องมอบหมายสิทธิ์ ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

4. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์ให้แก่ผู้ใช้งานไว้ในสถานที่ปลอดภัย

5. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิ์พิเศษที่ได้รับด้วยว่า การเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

6. ผู้ใช้บริการต้องรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์และต้องปฏิบัติตามอย่างเคร่งครัด

ระบบบริหารจัดการรหัสผ่าน (Password management system)

1. ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

2 ระบบบริหารจัดการรหัสผ่าน ต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติเพื่อยืนยันรหัสผ่านใหม่ที่ตั้งขึ้น

3 ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น เช่น ไม่ใช้ ชื่อ นามสกุล วันเกิด หมายเลขโทรศัพท์ คำจากพจนานุกรม เป็นต้น

4 ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ 6 เดือน

5 ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการเข้าสู่ระบบงาน (Login) เข้าใช้งานระบบงานเป็นครั้งแรก

6 ระบบบริหารจัดการรหัสผ่าน ต้องสามารถระบุข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งานได้ เช่น รหัสผ่าน มีความยาวของตัวอักขระน้อยกว่าที่กำหนด มีชื่อผู้ใช้งานอยู่ในรหัสผ่าน เป็นต้น

7. ระบบบริหารจัดการรหัสผ่าน ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้น กำลังใส่ข้อมูลบันทึกเข้าสู่ระบบงาน (Login) เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น

8. ระบบบริหารจัดการรหัสผ่าน ต้องมีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้ว เพื่อตรวจสอบไม่ให้ นำกลับมาใช้ใหม่ตามระยะเวลาที่เหมาะสม

9. การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

10. ระบบบริหารจัดการรหัสผ่าน ควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ และ/หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น โดยการเข้ารหัสข้อมูลการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

1. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์

2. ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ สำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

3. ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น

4. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่น และควรกำหนดรหัสผ่านที่แตกต่างกัน

5. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง และกำหนดให้ ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

1. ผู้ดูแลระบบดำเนินการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

2. ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิ์ในระดับสูง เช่น สิทธิ์ในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

3. ผู้ดูแลระบบทบทวนสิทธิ์ตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

4. ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิ์ในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

5. ผู้ดูแลระบบต้องดำเนินการตรวจสอบสิทธิ์และติดตามการใช้งานตามสิทธิ์ที่ได้รับของแต่ละระบบ

6. ผู้ดูแลระบบต้องกำหนดให้มีการเพิกถอนสิทธิ์หรือระงับการใช้งานของแต่ละสิทธิ์แตกต่างกันไปตามหน้าที่ที่รับผิดชอบในแต่ละระบบ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

การใช้งานบริการระบบเครือข่าย

การใช้งานบริการระบบเครือข่ายมีแนวทางปฏิบัติ ดังนี้

1. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของสหกรณ์

2. สหกรณ์ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไร ผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

3. ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาตการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิ์ของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว สหกรณ์ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

4. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของสหกรณ์

5. สหกรณ์ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธิ์นี้ให้กับผู้อื่นไม่ได้

6. บัญชีผู้ใช้งาน (User Account) ที่สหกรณ์ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

7. ผู้ใช้บริการระบบเครือข่ายของสหกรณ์ ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

8. การใช้งานบริการระบบเครือข่ายสหกรณ์ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

9. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

10. ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน

การระบุอุปกรณ์บนเครือข่าย

การระบุอุปกรณ์บนเครือข่ายมีแนวทางปฏิบัติ ดังนี้

1. ทำการระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Address และหมายเลขเครือข่าย (IP Address)

2. ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ (IP Address) และสถานที่ติดตั้ง

3. มีการใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดจะสามารถเข้าถึงเครือข่ายส่วนใดของสหกรณ์

4. มีการรักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อป้องกันการ เปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

5. อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

6. กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

7. จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายใน และ เครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย ทำการทบทวนแผนผังเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง

การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มีแนวทางปฏิบัติ ดังนี้

1. ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพ และ โดยการบันทึกเข้ามาใช้งาน

2 ทำการล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชัน (Configuration) ด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

3. ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

4. ผู้ดูแลระบบต้องกำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของ อุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

5. ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ เช่น สัปดาห์ละ 2 ครั้ง เป็นอย่างน้อย

6. บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติก่อน

7. มีการติดตั้งระบบป้องกันและตรวจสอบการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์อย่างปลอดภัย เช่น การใช้ระบบชีวภาพ (Biometric) หรือ สมาร์ทการ์ด (Smart card) หรือติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม หรือวิธีการอื่นที่มีความปลอดภัย

การแบ่งแยกเครือข่าย

การแบ่งแยกเครือข่าย มีแนวทางปฏิบัติ ดังนี้

1. สหกรณ์แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

2. ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการผู้ใช้งานและระบบงานต่าง ๆ ของสหกรณ์

3. ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่งจะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

4. มีการควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อย และป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณดักแอบดูข้อมูลบนเครือข่ายหรืออื่นๆ โดยไม่ได้รับอนุญาต

5. มีการใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

6. มีการกรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

7. มีการใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอกสหกรณ์ ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของสหกรณ์

8. มีการแยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่น ๆ ของสหกรณ์

9. มีการแยกกลุ่มเครือข่ายเป็น 4 ประเภทใหญ่ๆ คือ

(1) ระบบเครือข่ายภายใน (Local Area Network : LAN)

(2) ระบบเครือข่ายภายนอก (Extranet)

(3) ส่วนที่มีความสำคัญสูง (DMZ Zone : Demilitarized Zone) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

(4) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่าง ๆ ของสหกรณ์ (Intranet)

10. มีการจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็น ปัจจุบันหรืออย่างน้อยปีละครั้ง

การควบคุมการเชื่อมต่อทางเครือข่าย

การควบคุมการเชื่อมต่อทางเครือข่ายมีแนวทางปฏิบัติ ดังนี้

1. มีการตรวจสอบและจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย ที่สอดคล้องกับนโยบายควบคุมการเข้าถึงและข้อกำหนดของระบบงานที่ได้ระบุไว้

2. มีการจำกัดสิทธิ์และตามหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเชื่อมต่อเข้าสู่ระบบเครือข่ายสหกรณ์

3. มีการระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่ายสหกรณ์

4. มีการควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายสหกรณ์ โดยไม่ได้รับอนุญาต

5. มีการใช้ไฟร์วอลล์ทำการกรองข้อมูลที่ไหลเวียนในเครือข่าย ให้เป็นไปตามหรือสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายที่ได้กำหนดไว้

6. มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานต่าง ๆ ของสหกรณ์ อาทิ ระบบงานที่ใช้ในการส่งข้อความ (Messaging applications) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบงานสำหรับการโอนย้ายไฟล์ ระบบงานต่าง ๆ สำหรับใช้งานภายในสหกรณ์

7. มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน ตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

8. การเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสหกรณ์ จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก ซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

9. ทำการติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของ สหกรณ์ ในลักษณะที่ผิดปกติ

10. มีการป้องกันหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่าย (IP Address) ภายในสหกรณ์มิ ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

11. ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในสหกรณ์ เพื่อให้สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็นหรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้จัดการสหกรณ์ก่อนดำเนินการ

12. กำหนดระยะเวลาที่แน่นอนของการเชื่อมต่อจากระยะไกล เช่น ให้ใช้ในระยะเวลา 7 วัน และหลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

การควบคุมการจัดเส้นทางบนเครือข่าย

การควบคุมการจัดเส้นทางบนเครือข่ายมีแนวทางปฏิบัติ ดังนี้

1. มีการใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่าย (IP Address) ทั้งต้นทางและปลายทางและควบคุมการไหลของข้อมูลผ่านเครือข่ายต่าง ๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

2. มีการควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่าย (IP Address)

3. มีการกำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อ Domain Name เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

4. จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

5. มีการกำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่ายสหกรณ์

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการที่มีความมั่นคงปลอดภัย ซึ่งเริ่มตั้งแต่การลงทะเบียน การกำหนดสิทธิ์ การบริหารจัดการรหัสผ่าน และการทบทวนสิทธิ์ต่าง ๆ รวมถึงข้อกำหนด เกี่ยวกับการอนุญาตให้เข้าใช้และกำหนดรายละเอียดอื่น ๆ เพิ่มเติม โดยมีแนวทางปฏิบัติดังนี้

1. ผู้ใช้งานระบบปฏิบัติการต้องได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษร
2. ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
3. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อให้โปรแกรมทำการปิดหน้าจอภาพเมื่อไม่มีการใช้งาน หากภายหลังต้องการใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
4. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง
5. มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน 3 ครั้ง ระบบจะทำการจำกัดสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีกจนกว่าผู้ดูแลระบบจะดำเนินการปลดการจำกัดสิทธิให้
6. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน
7. ผู้ใช้งานต้องทำการบันทึกออกจากระบบ (Logout) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
8. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
9. ซอฟต์แวร์ที่มีลิขสิทธิ์ของสหกรณ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว
10. ซอฟต์แวร์ที่สหกรณ์จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
11. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของสหกรณ์ เพื่อหาประโยชน์ส่วนตัว
12. ในกรณีที่ผู้ใช้งานสร้างหน้าเว็บบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม

13. ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ในการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอน ทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

1. มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบบัญชีของเจ้าหน้าที่ทางเทคนิคอื่นๆ เป็นต้น

2. ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ยืนยันตัวตนที่แตกต่างกัน

3. ผู้ใช้งานต้องทำการพิสูจน์ยืนยันตัวตนทุกครั้ง ก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สหกรณ์โดยใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

4. ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูง ต้องจัดให้มีการพิสูจน์ยืนยันตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูง เช่น ใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพ (การใช้ลายนิ้วมือ ม่านตา ฝ่ามือ เสียง)

5. ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิ์การเข้าถึงระบบปฏิบัติการ จากผู้จัดการสหกรณ์หรือประธานคณะกรรมการดำเนินการสหกรณ์เท่านั้น

6. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

7. ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

8. ผู้ใช้งานต้องบันทึกเข้าระบบ (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และทำการบันทึกออกจากระบบ (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

การใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วโดยมีแนวทางปฏิบัติ ดังนี้

1. มีการจัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

2. มีการจำกัดผู้ที่สามารถใช้งานโปรแกรมอรรถประโยชน์และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้

3. ผู้ใช้งานที่ต้องการใช้งานโปรแกรมอรรถประโยชน์ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องมีการลงนามเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

4. การใช้งานโปรแกรมอรรถประโยชน์ จะต้องได้รับอนุญาตให้ใช้งานตามระดับสิทธิ์ในการใช้งานที่สหกรณ์กำหนดไว้แล้ว โดยจะได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

5. จำเป็นต้องทำการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ทุกครั้ง แม้จะเป็นการใช้งานเพียงชั่วคราว

6. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ เพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

7. มีการเก็บบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์

8. มีการยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์ที่ไม่มีความจำเป็นในการใช้งานแล้ว

9. ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

การหมดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศยุติตัวเองลง เมื่อไม่มีการใช้งานในช่วงเวลาหนึ่ง โดยมีแนวทางปฏิบัติ ดังนี้

1. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ เช่น ระบบงาน และอุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงการปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา 20 นาที

2. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์ ทำการพักหน้าจอหลังจากที่ไม่มีกิจกรรรมการใช้งานในช่วงระยะเวลา 10 นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

3. กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์สำหรับระบบที่มีความเสี่ยงสูง จะต้องมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

4. กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์สำหรับระบบที่มีความสำคัญสูง จะต้องมีการตัดและหมดเวลาการใช้งาน โดยมีกำหนดให้ไม่เกิน 1 ชั่วโมงต่อการพิสูจน์ยืนยันตัวตนเข้าใช้งาน

5 ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

การจำกัดการเข้าถึงสารสนเทศ

ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและเงื่อนไข (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติ ดังนี้

1. ผู้ดูแลระบบต้องป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อคที่ตัวเครื่อง การพิสูจน์ยืนยันตัวตน เป็นต้น

2. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ

3. ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

4. เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง เป็นต้น

5. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้บริการและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(5) ควรเปลี่ยนรหัสผ่านของข้อมูลหรือระบบที่มีลำดับความสำคัญตามระยะเวลาที่กำหนด

6. มีการใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

7. มีการลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัด หรือให้สิทธิ์การเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน เช่น การให้สิทธิ์ในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

8. มีการควบคุมหรือจำกัดสิทธิ์การเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง โดยควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่าง ๆ ที่จำเป็นต้องใช้งานเท่านั้น

9. มีการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้อง และจำเป็นสำหรับการนำไปใช้งานเท่านั้น

10. มีการแสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

11. มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่เข้าสู่ระบบงาน (Login) เสร็จแล้ว

12. มีข้อความแสดงเตือนห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

13. มีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใดๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ

14. มีการตรวจสอบข้อมูลการเข้าสู่ระบบงาน (Login) หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

15. มีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งาน ในลักษณะที่เปิดเผยข้อมูล ภายในของระบบงาน

16. มีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการเข้าสู่ระบบงาน (Login) ผิด

17. มีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการเข้าสู่ระบบงาน (Login) ผิดเกินกว่าจำนวนครั้งที่กำหนด

18. มีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามเข้าสู่ระบบงาน (Login) แต่ผิดพลาดเป็นจำนวนหลายครั้ง

19. มีการบันทึกข้อมูลการเข้าสู่ระบบงาน (Login) ทั้งที่สำเร็จและไม่สำเร็จ

20. มีการจำกัดช่วงระยะเวลาที่นานที่สุด ที่ผู้ใช้งานจะต้องเข้าสู่ระบบงาน (Login) เข้าใช้งานให้สำเร็จ

21. มีการแสดงวันเวลาของการเข้าสู่ระบบงาน (Login) ครั้งที่แล้ว (ทั้งสำเร็จและไม่สำเร็จ)

ระบบที่ไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อการปฏิบัติงานของสหกรณ์

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติในการดูแลและรักษาความมั่นคงปลอดภัยระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อการปฏิบัติงานของสหกรณ์ โดยจำเป็นต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ รวมทั้งต้องควบคุมการเข้าถึงโดยการเข้าผ่านอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกสหกรณ์ โดยมีวิธีการปฏิบัติดังนี้

1. ต้องมีการระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวนหรือมีผลกระทบสูงต่อสหกรณ์

2. ทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์เครื่องหนึ่งต่างหาก

3. มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูง กับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า เช่น ความเสี่ยงในการใช้เครื่อง ๆ เดียวกันในการให้บริการ

4. มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

5. มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกสหกรณ์ที่เกี่ยวข้องกับระบบดังกล่าว

6. ทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก ตามข้อกำหนดที่ตั้งค่าไว้ในไฟร์วอลล์

การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

1. มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์พกพา

2. สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกสหกรณ์ เป็นต้น

3. ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาตด้วยการเข้ารหัสข้อมูล

4. ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์คอมพิวเตอร์

5. สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ

6. มีการควบคุมการเข้าถึงระบบงานของสหกรณ์จากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตสาธารณะ

7. มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของสหกรณ์จากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา

8. มีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของสหกรณ์

9. ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงาน ภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ สหกรณ์ จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้า - ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการ ลงนามอย่างเป็นลายลักษณ์อักษร

10. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกัน เช่น พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area) เป็นต้น

การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการ ระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติ ดังนี้

1. มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ของสหกรณ์ ที่จำเป็นต้องปฏิบัติงานสหกรณ์จากภายนอกสำนักงานหรือจากระยะไกล

2 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

3. ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการ และต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

4. ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ยืนยันตัวตนก่อนเข้าใช้งาน

5. มีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

6 มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

7. มีการป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลกับระบบงานต่าง ๆ ภายในสหกรณ์

8. มีการกำหนดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันระหว่างสหกรณ์กับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

9. ไม่อนุญาตให้ครอบครัวหรือเพื่อนของผู้ปฏิบัติงานจากระยะไกล เข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของสหกรณ์

10. มีการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์จากระยะไกล รวมทั้งมาตรการควบคุมการใช้บริการเครือข่ายไร้สายจากที่อื่น ทั้งนี้เพื่อป้องกันการเข้าถึงระบบหรือข้อมูลของสหกรณ์โดยไม่ได้รับอนุญาต

11. มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล เพื่อป้องกันการโต้แย้งกันว่าใครเป็นเจ้าของทรัพย์สินทางปัญญานั้น

12. มีการสงวนสิทธิ์ในการเข้าถึงอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์จากระยะไกล เช่น เพื่อทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในอุปกรณ์นั้น เพื่อทำการตรวจสอบข้อมูลในอุปกรณ์สำหรับการดำเนินการสอบสวนกรณีที่มีเหตุเกิดขึ้น

13. มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์จากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

14. มีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น เช่น ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอลล์ในอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์จากระยะไกล

15. มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูลและอุปกรณ์สื่อสาร

16. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสหกรณ์จากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยสหกรณ์

17. มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่าง ๆ ที่ใช้งานจากระยะไกล

18. มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

19. มีการตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

วิธีการบริหารจัดการการเข้าถึงของผู้ใช้งานมีวิธีการปฏิบัติ ดังนี้

1. กำหนดขั้นตอนปฏิบัติของการลงทะเบียนเจ้าหน้าที่ใหม่อย่างเป็นทางการ ตามความจำเป็นโดยผู้ใช้งานเป็นผู้ร้องขอเพื่อเข้าใช้ระบบงาน ซึ่งมีผู้จัดการสหกรณ์เป็นผู้ให้การรับรองและผู้ดูแลระบบเป็นผู้บริหารจัดการบัญชีผู้ใช้งาน

2. ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกต้องทำภายใน 24 ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน 7 วัน

3. กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต ระบบงานของสหกรณ์ เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

4. ผู้ใช้ต้องลงนามรับทราบสิทธิ์ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด รวมทั้งเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

วิธีการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน

วิธีการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน มีวิธีการปฏิบัติ ดังนี้

1. ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

2. มีการกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน

3. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุดต้องมีการพิจารณาการควบคุม ผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(1) ต้องได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้น ๆ โดยนำเสนอผู้จัดการสหกรณ์อนุมัติ

(2) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(3) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(4) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย

วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย มีวิธีการปฏิบัติ ดังนี้

1. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 6 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลขและสัญลักษณ์เข้าด้วยกัน)

2. ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคล ที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

3. ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

4. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่

5. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

6. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ ให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้ต้องเป็นไปอย่างปลอดภัย

วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ มีวิธีการปฏิบัติ ดังนี้

1. การจัดแบ่งประเภทของข้อมูล ประกอบด้วย

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ยุทธศาสตร์/กลยุทธ์ บุคลากร รายงานกิจการ แผนงานงบประมาณ ข้อมูลการเงินและบัญชี และข้อมูลระบบบริหารจัดการ (Back Office)
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลสมาชิกหรือผู้รับบริการ ข้อมูลระบบงานของสหกรณ์

2. การจัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทข้างต้น ดังนี้
   - ข้อมูลที่มีระดับความสำคัญมากที่สุด
   - ข้อมูลที่มีระดับความสำคัญปานกลาง
   - ข้อมูลที่มีระดับความสำคัญน้อย
3. การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทข้างต้น ดังนี้ ลับที่สุด ลับมาก ลับ
4. การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทข้างต้น ดังนี้
   - สามารถเข้าถึงได้เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ
   - สามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานแล้วเท่านั้น
   - สามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
   - สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

5 การกำหนดเวลาการเข้าถึง ดังนี้
   - การเข้าถึงสารสนเทศในเวลาทำการ (08.30 – 16.30 น.)
   - การเข้าถึงสารสนเทศนอกเวลาทำการ (นอกช่วงเวลา 08.30 – 16.30 น.)
   - การเข้าถึงในช่วงเวลาวันหยุดทำการ (วันหยุดทำการ และวันหยุดนขัตฤกษ์)
   - การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

6 การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้
   - ระบบแลน (LAN) ในลักษณะ Client Server
   - ระบบอินทราเน็ต (Intranet) ในลักษณะ Web Base Application
   - ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application
   - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

ตารางสรุปแนวปฏิบัติในการเข้าถึงข้อมูลสารสนเทศของสหกรณ์มีรายละเอียด ดังนี้

เวลาการเข้าถึง	ประเภทข้อมูลสารสนเทศ	ระดับความสำคัญ	ระดับชั้นความลับ	ระดับชั้นการเข้าถึง	ช่องทาง
การเข้าถึงสารสนเทศใน เวลาทำการ (08.30 – 16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบแลน (LAN) - ระบบอินทราเน็ต (Intranet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงสารสนเทศนอกเวลาทำการ (นอกช่วงเวลา 08.30 – 16.30 น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงในช่วงเวลาวันหยุดทำการ (วันหยุดทำการ และวันหยุดนขัตฤกษ์)	- ด้านการบริหาร - ด้านการให้บริการ	- ปานกลาง - น้อย		- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึง และ จำนวนระยะเวลาการเข้าถึง)	- ด้านการบริหาร - ด้านการให้บริการ	มากที่สุด	ลับที่สุด	- เฉพาะผู้มีสิทธิ์สูงสุดในการบริหารจัดการระบบสารสนเทศ - เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิ์จากเจ้าของระบบงานแล้วเท่านั้น	- ระบบแลน (LAN) – ระบบอินทราเน็ต (Intranet)

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก (Outsource)

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูลความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้นเพื่อให้การควบคุมการปฏิบัติงานของหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสหกรณ์เป็นไปอย่างมั่นคงปลอดภัย มีแนวปฏิบัติดังนี้

การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsource)

1. การคัดเลือกผู้ให้บริการ ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

2. ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) ระบุผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ (source code) ในการพัฒนาซอฟต์แวร์ อย่างชัดเจน

3. กำหนดขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลาย-ลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนา หรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ ขั้นตอนในการโอนย้ายระบบงาน การส่งมอบงาน และได้รับการอนุมัติจากคณะกรรมการดำเนินการสหกรณ์

4. จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

5. มีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากคณะกรรมการดำเนินการสหกรณ์ทุกครั้ง

6. ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

7. ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

8. ฐานข้อมูลของระบบบัญชีคอมพิวเตอร์ทุกระบบต้องสามารถใช้ซอฟแวร์ในการดึงข้อมูลและส่งออกข้อมูลได้หลากหลายตามต้องการ

9. ผู้ให้บริการต้องมอบเอกสารโครงสร้างข้อมูล (Data structure) และคู่มือการปฏิบัติงานให้ครบทุกระบบงานไว้แก่สหกรณ์ รวมถึงการปรับปรุงให้เป็นปัจจุบันเสมอหากมีการพัฒนาหรือเปลี่ยนแปลงโปรแกรม

10. พิจารณาวางแผนดำเนินเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่สหกรณ์จำเป็นต้องเปลี่ยนไปใช้ระบบงานใหม่

แนวปฏิบัติในการควบคุมผู้ให้บริการภายนอก (Outsource)

1. ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของสหกรณ์ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้จัดการสหกรณ์หรือประธานกรรมการดำเนินการสหกรณ์

2. ดำเนินการเพิกถอน ลบ หรือเปลี่ยนสิทธิการเข้าถึงระบบงานและรหัสผ่านของผู้ให้บริการที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

3. กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

4. การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อและอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น และจะต้องแจ้งให้ผู้รับผิดชอบหรือผู้ดูแลระบบของสหกรณ์ทราบล่วงหน้าก่อนทุกครั้ง ซึ่งจะต้องระบุวันเวลาระยะเวลาในการทำงานให้ชัดเจน

5. ในกรณีที่หน่วยงานภายนอกมีความจำเป็นต้องสำเนาฐานข้อมูลทุกประเภทออกจากสหกรณ์ จะต้องจัดทำหนังสือขอความเห็นชอบจากประธานคณะกรรมการดำเนินการสหกรณ์ล่วงหน้าก่อนทุกครั้ง โดยจะต้องระบุเหตุผลในการนำไปใช้งานอย่างชัดเจนและต้องรับผิดชอบความเสียหายที่อาจเกิดขึ้นด้วย

การควบคุมการติดตั้งซอฟต์แวร์ใหม่ในระบบสารสนเทศที่ให้บริการ

1. ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของสหกรณ์เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

2. ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้วหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของสหกรณ์

3. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนการดำเนินงาน

4. ไม่ควรติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

5. กำหนดให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

6. กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

7. ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

8. ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม และขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

9. ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบสารสนเทศใหม่

1. แจ้งให้ผู้ที่เกี่ยวข้องระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบใหม่เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลง

2. มีการสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

3. กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศ โดยให้มีการบันทึกดังต่อไปนี้

(1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

(2) สถานที่ติดตั้ง

(3) เครื่องที่ติดตั้ง

(4) ผู้ผลิตซอฟต์แวร์

(5) ข้อมูลสาหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

แนวปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานของสหกรณ์ (Change Management)

การควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานของสหกรณ์มีวัตถุประสงค์ เพื่อให้ระบบงานคอมพิวเตอร์ของสหกรณ์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง มีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงที่เกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ (integrity risk) โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอ จนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

1. การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร (อาจเป็น electronic transaction เช่น Email เป็นต้น) และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หัวหน้าฝ่ายคอมพิวเตอร์ เป็นต้น
2. มีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง
3. มีการสอบทานกฎเกณฑ์ของระเบียบที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามระเบียบของสหกรณ์

การปฏิบัติงานพัฒนาระบบงาน

1. ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน(develop environment) ออกจากส่วนที่ใช้งานจริง (production environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้การแบ่งแยกส่วนตามที่กล่าว อาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่อง คอมพิวเตอร์เดียวกันก็ได้
2. ผู้ที่ร้องขอรวมทั้งผู้ใช้งานที่เกี่ยวข้องควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
3. ควรตระหนักถึงระบบรักษาความปลอดภัย (security) และเสถียรภาพการทำงาน (availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนาหรือการแก้ไขเปลี่ยนแปลง

การทดสอบระบบงาน

1. ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้อง ต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

2. ในระบบงานที่สำคัญควรมีหน่วยงานหรือทีมงานอิสระเข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบก่อนที่จะโอนย้ายไปใช้งานจริง

การโอนย้ายระบบงานเพื่อใช้งานจริง

1. การโอนย้ายข้อมูลหรือโปรแกรมในระบบงานที่พัฒนาเพื่อใช้งานจริง ต้องตรวจสอบการโอนย้ายให้ถูกต้องครบถ้วนเสมอ

2. ก่อนการใช้งานระบบงานใหม่ที่พัฒนาหรือปรับปรุงแก้ไข ต้องจัดให้มีการเปรียบเทียบยอดระหว่างระบบงานเดิมกับระบบงานใหม่

การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงานและจัดเก็บรุ่น (Version)

การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงานและจัดเก็บรุ่น (Version) ของระบบงานที่ได้รับการพัฒนา

1. ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

2. ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้าง ข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารตามที่กล่าวในที่ปลอดภัย และสะดวกต่อการใช้งาน

3. ต้องจัดเก็บโปรแกรม version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

การทดสอบหลังการใช้งาน (Post - Implementation Test)

การทดสอบหลังการใช้งานในระบบงาน (Post – Implementation Test) กำหนดให้มีการทดสอบระบบงานได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน

การสื่อสารการเปลี่ยนแปลง

ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

การใช้ Internet Account หรือรหัสผ่านในการใช้งานอินเทอร์เน็ต มีวิธีการปฏิบัติ ดังนี้

1. ผู้ใช้งานต้องลงทะเบียนเพื่อขอใช้งานอินเทอร์เน็ตจากผู้ดูแลระบบก่อน โดยต้องยอมรับและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสหกรณ์อย่างเคร่งครัด

2. ผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานอินเทอร์เน็ตได้ จะได้รับบัญชีผู้ใช้งาน (Account) ซึ่งประกอบด้วย รหัสผู้ใช้งานและรหัสผ่าน (Password) เพื่อเข้าใช้งานอินเทอร์เน็ต

3. ผู้ใช้งานต้องไม่ใช้บัญชีผู้ใช้งาน (Account) ของผู้อื่นโดยไม่ได้รับความยินยอมในการเข้าใช้งานอินเทอร์เน็ตของสหกรณ์ โดยจะต้องบัญชีผู้ใช้งาน (Account) ที่เป็นของตนเองในการแสดงตนเข้าใช้งานอินเทอร์เน็ตตามสิทธิ์ที่ได้รับเท่านั้น

4 ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่นในการใช้งานอินเทอร์เน็ต ให้ทำการบันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งานและเปลี่ยน Password ใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

5. ผู้ใช้งานต้องเป็นผู้รับผิดชอบบัญชีผู้ใช้งาน (Account) ที่สหกรณ์จัดสรรให้ ดังนั้นผู้ใช้งาน (ผู้อนุญาตและผู้ได้รับอนุญาต) ต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากการใช้งานบัญชีผู้ใช้งานของผู้ใช้งานนั้น ๆ ร่วมกันเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

6. ผู้ใช้งานควรทำการเปลี่ยนรหัสผ่าน (Password) ใหม่ทันที หากถูกเปิดเผยหรือสงสัยว่าถูกผู้อื่นนำไปใช้ โดยรหัสผ่าน (Password) ที่ตั้ง ควรจะประกอบด้วย ตัวหนังสือ ตัวเลข และอักขระพิเศษ เพื่อให้ยากต่อการคาดเดา

7. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุก ๆ 6 เดือน หรือตามที่ผู้ดูแลระบบกำหนด

8. ผู้ใช้งานต้องทำการออกจากระบบคอมพิวเตอร์ (Logout) เมื่อเลิกใช้งาน หรือเมื่อไม่อยู่ที่หน้าจอคอมพิวเตอร์นานเกิน 15 นาที

9. ผู้ดูแลระบบมีสิทธิ์ระงับบัญชีผู้ใช้งาน (Account) หากผู้ใช้งานไม่มีการใช้งานเป็นเวลา 30 วัน และถ้าไม่มีการติดต่อขอใช้งานเป็นเวลา 90 วันนับจากวันที่ระงับการใช้งาน ผู้ดูแลระบบจะยกเลิกบัญชีผู้ใช้งานดังกล่าวทันที

การใช้งานอินเทอร์เน็ต

การใช้งานอินเทอร์เน็ต มีวิธีการปฏิบัติ ดังนี้

1. การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ควรเชื่อมต่อผ่านระบบรักษาความมั่นคง ปลอดภัยที่ สหกรณ์ จัดสรรไว้เท่านั้น

2. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ สหกรณ์ ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ ดังต่อไปนี้

(1) เพื่อก่อให้เกิดความเสียหายแก่สหกรณ์ และบุคคลอื่น หรือละเมิดสิทธิ์ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลส่วนบุคคลของผู้อื่น การแสดง ความเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

(2) เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์ เช่น การจำลอง Mail Server โดยมีการใช้อินเทอร์เน็ตของสหกรณ์ในการส่ง mail จำนวนมาก การจำลอง Web Server เพื่อจัดทำเว็บไซต์สำหรับค้าขายโดยมีการใช้อินเทอร์เน็ตของสหกรณ์ เป็นต้น

(3) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสมการใช้ข้อความที่สร้างความตื่นตระหนกกับสังคมโดยรวมบนเว็บบอร์ด เป็นต้น

(4) เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาต ซึ่งได้มาจากสหกรณ์หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

3. ผู้ใช้งานไม่ควรดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะการยึดครองช่องสัญญาณการสื่อสารข้อมูลตลอดเวลา (Consume Bandwidth) ผ่านอินเทอร์เน็ตในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวิดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องส่งข้อมูลที่มีขนาดใหญ่ ให้ติดต่อผู้ดูแลระบบดำเนินการเท่านั้น

4. ผู้ใช้งานที่มีความจำเป็นต้องนำเครื่องคอมพิวเตอร์โน้ตบุ๊กไปเชื่อมต่อเข้ากับอินเทอร์เน็ตนอกเหนือเครือข่ายอินเทอร์เน็ตของสหกรณ์ ต้องมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่มีการ ปรับปรุงซอฟต์แวร์ป้องกันให้มีความทันสมัยตลอดเวลา

5. ผู้ใช้งานควรแจ้งข้อเท็จจริงต่อผู้ดูแลระบบ หากพบเห็นการใช้อินเทอร์เน็ตในเครือข่ายของสหกรณ์ ไปในทางที่ไม่เหมาะสม หรือพบเห็นการบุกรุกหรือการละเมิดสิทธิ์ของสหกรณ์

6. ผู้ใช้งานไม่ควรดาวน์โหลด (download) ไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัย เช่น โปรแกรมรักษาจอภาพ เกมส์ และโปรแกรมที่ลงท้ายด้วย .exe หรือ .com หากมีความจำเป็นต้องดาวน์โหลด ต้องมีการตรวจสอบด้วยโปรแกรมป้องกันไวรัสก่อนการนำไปใช้ทุกครั้ง

แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

การสำรองข้อมูลและระบบคอมพิวเตอร์ ผู้ดูแลระบบหรือคณะทำงานที่เกี่ยวข้องจะต้องระบุแนวปฏิบัติสำหรับการจัดทำระบบสำรองข้อมูลที่ชัดเจน เพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

1. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ให้ดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองข้อมูลของสหกรณ์

2. ผู้ดูแลระบบ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตาม นโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศของสหกรณ์

3. ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

4. ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของสหกรณ์

5. มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ ความถี่ในการสำรองและจัดทำทะเบียนคุมข้อมูลชุดสำรอง

6. จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

7. ดำเนินการตามกระบวนการสำรองข้อมูล สำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

8. มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำหรับสถานที่ที่ใช้จัดเก็บข้อมูล

9. การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

10. กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบ ทั้งซอฟต์แวร์และข้อมูลในระบบสารสนเทศ ในกรณีมีข้อผิดพลาดเกิดขึ้นต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

11. ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหาสรุปผลการแก้ไขปัญหาและรายงานต่อผู้จัดการสหกรณ์หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการดำเนินงาน

12. ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

13. ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูล (Encrypted backup) ในการสำรองข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

14. ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

การปฏิบัติเกี่ยวกับการสำรองข้อมูล

การปฏิบัติเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติ ดังนี้

1. ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ ดังนี้

(1) Web servers : สำรองข้อมูลเผยแพร่บนเว็บไซต์ 1 ครั้งต่อเดือน

(2) Database servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ 1 ครั้งต่อสัปดาห์

(3) Firewall server : สำรองข้อมูล Rule ของ Firewall 1 ครั้งต่อเดือน

(4) Server อื่นๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่าง ๆ 1 ครั้งต่อเดือน

2 ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่

การทดสอบและการกู้คืนระบบ

สหกรณ์ต้องกำหนดแผนการทดสอบกู้คืนข้อมูล ตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้ว เพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไขพร้อมทั้งรายงานผลการแก้ไขสรุปผลการปฏิบัติงานต่อประธานคณะกรรมการดำเนินการสหกรณ์ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการดำเนินการสหกรณ์ทราบ

2. การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายของสหกรณ์ กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ดูแลระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

4. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ 1 ครั้ง

การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

สหกรณ์ต้องเตรียมการสำหรับจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถปฏิบัติงานในระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจโดยมีวิธีการปฏิบัติ ดังนี้

1. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

2. ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

3. ผู้ดูแลระบบต้องทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

4. ผู้ดูแลระบบต้องบันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึงประเภทปริมาณและหลักฐานสำหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

5. รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ควรมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบสารสนเทศของสหกรณ์ โดยมีหัวข้อสำคัญ ดังนี้

- การเตรียมการเบื้องต้น
- ผู้รับผิดชอบ
- มาตรการความปลอดภัยและแผนการดำเนินงาน ในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติ เมื่อเกิดความเสียหายหรือหยุดทำงาน

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

การประเมินผลกระทบที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

แนวทางในการประเมินระดับผลกระทบ โดยกำหนดการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ที่เกี่ยวกับผลกระทบต่อไปนี้

1. ผลกระทบด้านมูลค่าความเสียหายทางการเงินให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(1) ในกรณีมูลค่าความเสียหายทางการเงินไม่เกินหนึ่งล้านบาท ให้จัดเป็นผลกระทบระดับต่ำ

(2) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งล้านบาทแต่ไม่เกินหนึ่งร้อยล้านบาท ให้จัดเป็นผลกระทบระดับกลาง

(3) ในกรณีมูลค่าความเสียหายทางการเงินเกินกว่าหนึ่งร้อยล้านบาทขึ้นไป ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินมูลค่าความเสียหายทางการเงินตามวรรคหนึ่ง ให้คำนวณจากความเสียหายที่จะเกิดขึ้นในหนึ่งวัน และคำนวณความเสียหายโดยตรงเท่านั้น

2. ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย ให้จัดเป็นสามระดับโดยมีเกณฑ์ในการประเมิน ดังนี้

(1) ในกรณีที่ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ให้จัดเป็นผลกระทบระดับต่ำ

(2) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยตั้งแต่หนึ่งคนแต่ไม่เกินหนึ่งพันคน ให้จัดเป็นผลกระทบระดับกลาง

(3) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัยเกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคนให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัยตามวรรคหนึ่งให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน

3. ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับความเสียหายอื่นใดนอกจากในข้อ 2 หรือข้อ 4 ให้จัดเป็นสามระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(1) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบไม่เกินหนึ่งหมื่นคน ให้จัดเป็นผลกระทบระดับต่ำ

(2) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับกลาง

(3) ในกรณีจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับผลกระทบเกินกว่าหนึ่งแสนคน ให้จัดเป็นผลกระทบระดับสูง

ในการประเมินผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายตามวรรคหนึ่ง ให้คำนวณจากจำนวนของบุคคลดังกล่าวที่ได้รับผลกระทบในหนึ่งวัน และคำนวณความเสียหายโดยตรง เท่านั้น

4. ผลกระทบด้านความมั่นคงของรัฐ ให้จัดเป็นสองระดับ โดยมีเกณฑ์ในการประเมิน ดังนี้

(1) ในกรณีไม่มีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับต่ำ

(2) ในกรณีมีผลกระทบต่อความมั่นคงของรัฐ ให้จัดเป็นผลกระทบระดับสูง

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยมีเนื้อหาอย่างน้อย ดังนี้

(1) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง

(2) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบกิจการของสหกรณ์ หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้คณะกรรมการดำเนินการของสหกรณ์ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

2. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

(1) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

(2) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อย ปีละ 1 ครั้ง

(3) มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

(4) มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้

- ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
- ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อก (log) แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ
- ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

การประเมินสถานการณ์ความเสี่ยงและแนวทางปฏิบัติในระบบเทคโนโลยีสารสนเทศสหกรณ์

สถานการณ์ความเสี่ยงในระบบเทคโนโลยีสารสนเทศสหกรณ์ ที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของสหกรณ์ สามารถแยกเป็นภัยและความเสี่ยงต่าง ๆ ดังนี้

1. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) ได้แก่ เจ้าหน้าที่หรือบุคลากรของสหกรณ์ขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้ง ด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากรของสหกรณ์ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ดังนี้

(1) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(2) นำเสนอนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณาใน การประชุมดำเนินการสหกรณ์

(3) จัดทำนโยบายว่าด้วยการใช้งานคอมพิวเตอร์ทั่วไปและการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต เผยแพร่ผ่านเพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

2. ภัยที่เกิด Software

ภัยที่เกิดจาก Software เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหาย ให้แก่ระบบเทคโนโลยีสารสนเทศของสหกรณ์ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(1) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่ายทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(2) มีการติดตั้งซอฟต์แวร์ Antivirus ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) เพื่อดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของสหกรณ์ป้องกันและแก้ไขปัญหาใน

3. ภัยจากไฟไหม้ หรือระบบไฟฟ้า ดำเนินการดังต่อไปนี้

(1) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) และเครื่องสำรองไฟฟ้าฉุกเฉิน เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง โดยมีการสำรวจตรวจสอบระยะเวลาการ สำรองไฟ กรณีที่เกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่ สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(2) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายใน ห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัย เพื่อทราบ และรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(3) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟ ไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ รวมทั้งมีการจัดฝึกอบบรมการป้องกันอัคคีภัยทุกปี

4. ภัยจากน้ำท่วม (อุทกภัย)

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากน้ำท่วม (อุทกภัย) ดำเนินการดังนี้

(1) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(2) เมื่อเกิดน้ำขังหรือมีการรั่วซึมจากน้ำ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อย ๆ จนน่าจะเข้าสู่ภาวะวิกฤติต่อระบบการให้บริการของสหกรณ์ ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด

(3) ถอดเทป Backup ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย

(4) ดำเนินการตัดระบบน้ำและไฟฟ้าในห้องควบคุม ปิดเบรคเกอร์เครื่องปรับอากาศ เพื่อป้องกัน เครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(5) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ไว้ในชั้นที่สูงขึ้นไป เฉพาะส่วนที่เคลื่อนย้ายได้

(6) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้ งานได้ปกติหรือไม่และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

(7) เมื่อระบบไฟฟ้าใช้งานได้ตามปกติ ผู้ดูแลระบบและเจ้าหน้าที่ผู้เกี่ยวข้องช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์ทำหน้าที่แม่ข่าย มาติดตั้ง ณ ห้องควบคุมระบบเครือข่ายเดิม

(8) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบเครือข่ายว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(9) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้บริการได้ตามปกติ

5. ความเสี่ยงจากอุปกรณ์โครงสร้างพื้นฐานที่เก่าชำรุดล้าสมัย แนวทางปฏิบัติ

(1) ตรวจสอบอุปกรณ์ฯ เพื่อให้ใช้งานได้ตามปกติ

(2) ทำการบำรุงรักษา ทั้งเชิงป้องกัน และเชิงแก้ไข

(3) จัดหาอุปกรณ์ทดแทนอุปกรณ์ที่เสียหายใช้การไม่ได้ หรือไม่เหมาะกับเทคโนโลยีสมัยใหม่