นโยบายความปลอดภัยระบบสารสนเทศ

ในยุคปัจจุบัน ระบบสารสนเทศมีบทบาทสำคัญอย่างยิ่งต่อการดำเนินธุรกิจและชีวิตประจำวัน การใช้เทคโนโลยีดิจิทัลได้กลายเป็นส่วนหนึ่งของกระบวนการทำงานและการให้บริการของทุกองค์กร โดยเฉพาะอย่างยิ่งสำหรับ บริษัท เอส ไอเอส ดิสทริบิวชั่น (ประเทศไทย) จำกัด (มหาชน) (บริษัทฯ) ซึ่งดำเนินธุรกิจด้านเทคโนโลยี การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจึงเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อคุ้มครองข้อมูล ทรัพยากรระบบ และทรัพย์สินทางดิจิทัลของบริษัทฯ ให้ปลอดภัยจากภัยคุกคามทางไซเบอร์และการเข้าถึงโดยไม่ได้รับอนุญาต

ด้วยเหตุนี้ บริษัทฯ จึงได้กำหนด นโยบายความปลอดภัยสารสนเทศและแนวทางการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสอดคล้องกับกฎหมาย มาตรฐานสากล และแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศขององค์กร ไว้ดังรายละเอียดต่อไปนี้

1. นิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

1.1 แผนกฯ หมายถึง แผนกสารสนเทศ

1.2 ทรัพย์สิน หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของบริษัทฯ ภายใต้การกำกับดูแลของแผนกสารสนเทศ

1.3 ระบบเครือข่าย หมายถึง เครือข่ายคอมพิวเตอร์ของบริษัทฯ ภายใต้การกำกับดูแลของแผนกสารสนเทศ

1.4 ระบบสารสนเทศ หมายถึง ระบบสารสนเทศของบริษัทฯ ภายใต้การกำกับดูแลของแผนกสารสนเทศ

1.5 พนักงาน หมายถึง เจ้าหน้าที่ที่สังกัดแผนกสารสนเทศ

1.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ หมายถึง เจ้าหน้าที่ผู้รับผิดชอบด้านการให้บริการระบบเครือข่ายคอมพิวเตอร์

1.7 ผู้พัฒนาระบบสารสนเทศ หมายถึง เจ้าหน้าที่ของแผนกสารสนเทศที่มีหน้าที่ในการพัฒนาระบบสารสนเทศให้กับแผนกฯและหน่วยงานต่างๆภายในบริษัทฯ

2. บททั่วไป

2.1 นโยบายความปลอดภัยสารสนเทศนี้ถูกจัดทำขึ้นโดยคณะกรรมการความปลอดภัยระบบสารสนเทศ ซึ่งนโยบายฉบับนี้จะถูกทบทวน และปรับปรุงให้มีความทันสมัยทุกปี (หากมี)

2.2 นโยบายความปลอดภัยระบบสารสนเทศ ต้องได้รับการจัดทำเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้อำนวยการฝ่ายปฏิบัติการ และต้องเผยแพร่ให้พนักงานทุกคนทราบ

3. ความรับผิดชอบของผู้บริหารแผนกฯ

3.1 ผู้อำนวยการฝ่ายปฏิบัติการต้องเป็นผู้ลงนามอนุมัตินโยบายความปลอดภัยสารสนเทศ

3.2 ผู้อำนวยการฝ่ายปฏิบัติการต้องทบทวนนโยบาย และปรับปรุงให้ทันสมัยทุกปี (หากมี)

3.3 ผู้อำนวยการฝ่ายปฏิบัติการต้องเป็นผู้ผลักดันให้พนักงานของแผนกฯทุกคนตระหนักถึงความสำคัญในการรักษาความปลอดภัยของทรัพย์สินสารสนเทศของแผนกฯ

3.4 ผู้อำนวยการฝ่ายปฏิบัติการต้องเป็นผู้ผลักดันให้พนักงานของแผนกฯทุกคนปฏิบัติตามนโยบายความปลอดภัยสารสนเทศและตามกฎหมาย

3.5 ผู้อำนวยการฝ่ายปฏิบัติการต้องให้การสนับสนุนด้านทรัพยากรต่างๆ เพื่อให้การบริหารจัดการและให้บริการระบบเครือข่ายคอมพิวเตอร์มีความปลอดภัยและสอดคล้องกับนโยบายฉบับนี้

4. ด้านโครงสร้างความปลอดภัยของแผนกฯ

4.1 แผนกฯต้องมีคำสั่งแต่งตั้งคณะกรรมการความปลอดภัยระบบสารสนเทศเพื่อจัดทำร่างข้อกำหนดด้านความปลอดภัยของข้อมูลสารสนเทศบนระบบเครือข่ายคอมพิวเตอร์และเสนอลงนามต่อผู้อำนวยการฝ่ายปฏิบัติการ โดยคณะกรรมการชุดนี้มีหน้าที่หลักในการร่างข้อกำหนดด้านความปลอดภัยของข้อมูลสารสนเทศ และควบคุมพนักงานรวมไปถึงหน่วยงานภายนอกให้ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศฉบับนี้

4.2 ฝ่ายทรัพยากรบุคคลต้องจัดให้มีการลงนามข้อตกลงระหว่างพนักงานและแผนกฯว่าจะไม่เปิดเผยความลับของแผนกฯ และความลับของบริษัทฯต่อบุคคลภายนอก หากมิได้อนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการฝ่ายปฏิบัติการ

4.3 เพื่อให้เกิดความรวดเร็วในการแก้ไขปัญหา เมื่อมีเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์ควรมีรายชื่อสำหรับติดต่อประสานงานด้านความมั่นคงปลอดภัย เช่น ผู้ให้บริการอินเทอร์เน็ต ศูนย์ประสานงานด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น

4.4 หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์ต้องประเมินความเสี่ยงอันเกิดจากการเข้าถึงระบบเครือข่ายคอมพิวเตอร์โดยบุคคลภายนอก และมีมาตรการรองรับหรือแก้ไขที่ชัดเจน เป็นระยะๆตามที่กำหนด โดยอาจจะเป็นทุกๆ 6 เดือนก็ได้

4.5 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องแจ้งนโยบายในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ และขั้นตอนปฏิบัติการเข้าใช้งานห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ให้กับบุคคลภายนอกทราบก่อนอนุมัติให้ใช้งาน

5. ด้านการบริหารจัดการทรัพย์สินของแผนกฯ

5.1 แผนกฯ ต้องจัดทำบัญชีทรัพย์สินระบบเครือข่ายคอมพิวเตอร์ของแผนกฯ โดยระบุผู้รับผิดชอบในทรัพย์สินแต่ละชิ้นอย่างชัดเจน และจัดหมวดหมู่ทรัพย์สินตามระดับความสำคัญ ความลับ คุณค่า เพื่อหาวิธีการบริหารจัดการที่เหมาะสม

5.2 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องบริหารจัดการทรัพย์สินที่แยกตามหมวดหมู่ไว้แล้ว เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

6. ด้านความมั่นคงปลอดภัยของแผนกฯ ที่เกี่ยวข้องกับพนักงาน

6.1 หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์และฝ่ายทรัพยากรบุคคล ต้องกำหนดหน้าที่และความรับผิดชอบด้านความปลอดภัยระบบสารสนเทศเป็นลายลักษณ์อักษรสำหรับพนักงาน และ/หรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน

6.2 ฝ่ายทรัพยากรบุคคลและหน่วยงานภายในที่เกี่ยวข้องต้องตรวจสอบคุณสมบัติของผู้สมัครเข้าเป็นพนักงานใหม่โดยละเอียด เช่น ประวัติการทำงาน วุฒิการศึกษา และระดับความเสี่ยงในการเข้าถึงสารสนเทศ เป็นต้น

6.3 ฝ่ายทรัพยากรบุคคลและงานต่างๆของแผนกฯที่เกี่ยวข้องต้องกำหนดเงื่อนไขการจ้างงาน รวมไปถึงหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศ โดยพนักงานใหม่จะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานด้วย

6.4 แผนกฯต้องสร้างความตระหนักให้พนักงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกตระหนักถึงความปลอดภัย เกี่ยวกับลักษณะงานที่พนักงานต้องรับผิดชอบ

6.5 พนักงานและหน่วยงานภายนอกที่จะเข้ามาปฏิบัติงาน ต้องปฏิบัติตามนโยบายความปลอดภัยของแผนกฯ

6.6 พนักงานที่ฝ่าฝืนหรือละเมิดนโยบายด้านความปลอดภัยสารสนเทศของแผนกฯ ต้องถูกลงโทษตามกระบวนการทางวินัย

6.7 พนักงานที่ลาออกจากงานหรือถูกเลิกจ้างงาน ต้องคืนทรัพย์สินของแผนกฯที่อยู่ในความครอบครองของตน และถูกยกเลิกสิทธิ์ในการเข้าถึงทรัพย์สินหรือข้อมูลสารสนเทศ

7. ด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

7.1 งานบริการระบบเครือข่ายคอมพิวเตอร์ งานพัฒนาระบบสารสนเทศและแผนก General Affair ต้องจัดทำบริเวณรักษาความปลอดภัยและจัดให้มีการควบคุมการเข้า ออก เฉพาะผู้ได้รับอนุญาต รวมไปถึงการกำหนดบริเวณสำหรับบุคคลภายนอกในการเข้าถึงเพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย การก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศของแผนกฯ

7.2 แผนกฯ ต้องจัดทำแผนป้องกันอุบัติภัย เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่นๆทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้โดยเร็วที่สุด

7.3 พนักงานต้องจัดวางและป้องกันทรัพย์สินของแผนกฯ ให้ปลอดภัยจากภัยคุกคามด้านสิ่งแวดล้อม อันตรายต่างๆ รวมทั้งการเข้าถึงโดยไม่ได้รับอนุญาต

7.4 เพื่อลดความเสี่ยงในการล้มเหลวของระบบสนับสนุนการให้บริการระบบเครือข่าย แผนกฯต้องบำรุงรักษาระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบปรับอากาศ เป็นต้น ให้สามารถใช้งานได้อย่างต่อเนื่อง และมีระบบสำรองหากเกิดเหตุการณ์ที่ระบบสาธารณูปโภคหลักไม่สามารถใช้งานได้

7.5 อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานภายนอกแผนกฯ สายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ ต้องได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อสายสัญญาณ หรืออุปกรณ์ระบบเครือข่ายคอมพิวเตอร์นั้นๆ

7.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟท์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือเขียนทับ ก่อนที่จะทิ้งอุปกรณ์ดังกล่าวเพื่อป้องกันข้อมูลหากอุปกรณ์นั้นถูกนำกลับมาใช้อีกครั้ง

7.7 พนักงานต้องไม่นำทรัพย์สินสารสนเทศของแผนกฯออกไปภายนอกแผนกฯ ยกเว้นได้รับอนุญาต ซึ่งต้องปฏิบัติตามระเบียบการนำพัสดุออกภายนอกอาคารอย่างเคร่งครัด

8. ด้านการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของแผนกฯ

8.1 งานบริการระบบเครือข่ายคอมพิวเตอร์ต้องจัดทำระเบียบปฏิบัติด้านการให้บริการระบบเครือข่ายคอมพิวเตอร์เป็นลายลักษณ์อักษร และเผยแพร่ให้กับพนักงาน และผู้เกี่ยวข้องรับทราบ

8.2 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องควบคุมการให้บริการของหน่วยงานภายนอกให้ปฏิบัติตามข้อตกลงด้านความปลอดภัยที่ทำไว้ระหว่างแผนกฯและหน่วยงานภายนอก

8.3 แผนกฯ ต้องวางแผนความต้องการทรัพยากรสารสนเทศเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

8.4 ระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือติดตั้งใหม่ ต้องผ่านการตรวจสอบว่าไม่มีผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์โดยรวม ก่อนนำระบบนั้นมาใช้งาน

8.5 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องตรวจจับ ป้องกัน และกู้คืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีหรือโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่สามารถเคลื่อนย้ายจากหน่วยความจำคอมพิวเตอร์เครื่องหนึ่งไปยังหน่วยความจำคอมพิวเตอร์อีกเครื่องหนึ่งได้ด้วยตัวเอง) รวมทั้งมีการสร้างความตระหนักถึงอันตรายที่เกิดขึ้นจากโปรแกรมที่ไม่ประสงค์ดีเหล่านี้ รวมถึงเผยแพร่วิธีการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัยให้ผู้ใช้งานทราบด้วย

8.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องสำรองข้อมูลและทดสอบข้อมูลที่เก็บไว้อย่างสม่ำเสมอตามขั้นตอนการปฏิบัติงานเรื่องการสำรองข้อมูล

8.7 หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์ต้องบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ จัดระดับการให้บริการ กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆทางระบบเครือข่าย และดูแลรักษาระบบความปลอดภัยสำหรับระบบเครือข่ายและแอพพลิเคชั่นที่ใช้งานบนระบบเครือข่าย รวมทั้งข้อมูลสารสนเทศต่างๆที่ส่งผ่านทางระบบเครือข่ายคอมพิวเตอร์

8.8 งานบริการระบบเครือข่ายคอมพิวเตอร์ต้องมีวิธีการจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

8.9 พนักงานในแผนกฯ ทุกคนต้องปฏิบัติตามระเบียบปฏิบัติเรื่องการควบคุมเอกสาร

8.10 แผนกฯ ต้องกำหนดขั้นตอนปฏิบัติ และมาตรการรองรับ ในการแลกเปลี่ยนสารสนเทศ และซอฟท์แวร์ภายในแผนกฯ หรือระหว่างหน่วยงาน

8.11 ก่อนการเผยแพร่ข้อมูลออกสู่สาธารณะ ผู้รับผิดชอบในการเผยแพร่ข้อมูล ต้องตรวจสอบความถูกต้องของข้อมูลสารสนเทศ เพื่อข้อมูลมีความถูกต้อง ไม่ก่อให้เกิดความเข้าใจผิด อีกทั้งเมื่อเผยแพร่ออกไปแล้วต้องมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาตอีกด้วย

8.12 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ โดยเก็บข้อมูลดังนี้

8.12.1 ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย (Network Access Systems) (Dial up services)

8.12.2 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)

8.12.3 ข้อมูลอินเทอร์เน็ตที่เกิดจากการถ่ายโอนข้อมูลบนเครื่องให้บริการถ่ายโอนข้อมูล (FTP servers)

8.12.4 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ (Web servers)

8.12.5 ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

8.12.6 ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้ตามสิทธิ์ที่ได้รับ

9. ด้านการควบคุมการเข้าถึงทรัพย์สินสารสนเทศ

9.1 หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์และหัวหน้างานที่เกี่ยวข้องต้องมีการควบคุมและจำกัดสิทธิ์การใช้งานระบบตามความจำเป็นในการใช้งาน

9.2 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องบริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้ตามสิทธิ์ที่ได้รับ

9.3 ผู้ใช้งานต้องมีวิธีการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึง สามารถเข้าถึงทรัพย์สินสารสนเทศที่อยู่ในความรับผิดชอบของตนเองโดยไม่มีเจ้าหน้าที่ดูแลได้ เช่น เมื่อหยุดใช้งานเครื่องคอมพิวเตอร์ให้ทำการล็อคหน้าจอ หรือเมื่อออกจากห้องปฏิบัติงานให้ล็อคประตู เป็นต้น

9.4 ทรัพย์สินสารสนเทศที่สำคัญ ไม่ว่าจะเป็นเอกสาร หรือสื่อบันทึกข้อมูล ต้องไม่อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ หรืออยู่ในที่สาธารณะ พบเห็นได้ง่าย เป็นต้น

9.5 ก่อนการใช้งานระบบเครือข่ายคอมพิวเตอร์หรืออุปกรณ์บนระบบเครือข่าย จะต้องทำการระบุตัวตนผู้ขอใช้งานทุกครั้ง เพื่อทราบว่าใครเป็นผู้ขอใช้งานและสิทธิ์ในการใช้งาน

9.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์จะต้องการป้องกันการเข้าถึงพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ไม่ว่าจะเป็นจากทางกายภาพหรือผ่านระบบเครือข่าย

9.7 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องแยกระบบเครือข่ายออกเป็นกลุ่มของผู้ใช้งาน และกลุ่มของเครื่องแม่ข่ายที่ให้บริการระบบสารสนเทศ รวมไปถึงระบบสารสนเทศที่มีความสำคัญสูง เพื่อให้ง่ายต่อการจำกัดการเข้าถึงและบริหารจัดการความปลอดภัยระบบเครือข่ายคอมพิวเตอร์

9.8 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่าย เพื่อให้ข้อมูลสารสนเทศบนระบบเครือข่ายถูกจำกัดสิทธิ์ในการเข้าถึงจากผู้ใช้งานระบบเครือข่ายได้

9.9 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องมีการระบุตัวตน การควบคุมรหัสผ่าน และการจำกัดระยะเวลาในการเข้าถึงระบบปฏิบัติการ เช่น ระบบจะตัดเมื่อผู้ใช้งานไม่ได้ใช้งานมาเป็นระยะเวลาหนึ่ง เป็นต้น

9.10 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องควบคุมอุปกรณ์สื่อสารชนิดพกพา เช่น Notebook, PDA เป็นต้น และหาวิธีการป้องกันเพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากอุปกรณ์เหล่านี้ เมื่อถูกนำเข้ามาใช้งานในระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ

10. ด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

10.1 ผู้พัฒนาระบบสารสนเทศขึ้นมาใหม่ หรือปรับปรุงจากของเดิมที่มีอยู่แล้ว จะต้องระบุข้อกำหนดความปลอดภัยของระบบใหม่นี้ก่อนใช้งาน เพื่อผู้ที่ใช้งานจะไม่ทำให้ระบบนี้ใช้งานไม่ได้หรือก่อกวนระบบเครือข่ายคอมพิวเตอร์โดยรวม

10.2 ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำเข้าสู่กระบวนการประมวลผล และมีระบบตรวจสอบระหว่างการประมวลผลว่าเกิดความผิดพลาดหรือไม่ รวมทั้งตรวจสอบหลังจากที่ประมวลผลเรียบร้อยว่าข้อมูลสารสนเทศมีความถูกต้องหรือไม่ ก่อนนำไปใช้งาน

10.3 ผู้พัฒนาระบบสารสนเทศต้องควบคุมการติดตั้งซอฟท์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบบริการเสียหาย ผิดปกติ หรือไม่สามารถใช้งานได้ เช่น กรณีที่จะติดตั้งอุปกรณ์หรือพัฒนาระบบใดๆ ที่จะส่งผลกับระบบโดยรวม จะต้องตัดตัวเองออกจากระบบโดยรวมเสียก่อน หรือทำการทดสอบในระบบจำลองก่อนที่จะนำมาใช้กับระบบจริง เป็นต้น

10.4 ผู้พัฒนาระบบต้องหลีกเลี่ยงการนำข้อมูลจริงที่ใช้อยู่บนระบบให้บริการมาทดสอบระบบ หากมีความจำเป็นต้องนำมาใช้ให้ทำการควบคุม เช่น การลบข้อมูลส่วนตัว การลบบางส่วนของข้อมูลที่เป็นความลับ เป็นต้น

10.5 หัวหน้างานพัฒนาระบบสารสนเทศต้องมีระบบการจำกัดการเข้าถึงซอร์สโค้ดที่ระบบให้บริการอยู่ เพื่อป้องกันการเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ได้รับอนุญาตหรือไม่ได้เจตนา

10.6 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องมีวิธีปฏิบัติในการควบคุมหรือเปลี่ยนแปลงแก้ไขระบบสารสนเทศ โดยต้องมีการตรวจสอบทางเทคนิคว่าระบบยังทำงานดีอยู่หรือไม่หลังจากการเปลี่ยนแปลงแก้ไขระบบสารสนเทศเรียบร้อยแล้ว

10.7 หลีกเลี่ยงการแก้ไขซอฟท์แวร์ที่มาจากผู้ผลิต หากมีความจำเป็น ต้องมีการควบคุมการแก้ไขอย่างเข้มงวด

10.8 หัวหน้างานพัฒนาระบบสารสนเทศต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่สารสนเทศจะรั่วไหลออกไป เพื่อไม่ให้ผู้อื่นนำข้อมูลสารสนเทศนี้ไปใช้งานโดยมิชอบได้

10.9 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องวางแผนประเมินความเสี่ยงของระบบ ทำการทดสอบ และกำหนดมาตรการป้องกันช่องโหว่ของระบบ

11. ด้านการบริหารจัดการความเสี่ยงด้านความปลอดภัยของระบบสารสนเทศ

11.1 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องจัดทำรายงานผลประเมินความเสี่ยง พร้อมคำแนะนำในการลดความเสี่ยงเหล่านั้น เพื่อให้ผู้บริหารพิจารณาทุก 6 เดือน โดยมีข้อมูลครอบคลุมอย่างน้อยตามหัวข้อดังนี้

11.1.1 ด้านการใช้งานระบบสารสนเทศที่ไม่ถูกต้องตามนโยบาย ประกาศ หรือระเบียบปฏิบัติ

11.1.2 ด้านภัยคุกคามจากไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ และมัลแวร์

11.1.3 ด้านภัยคุกคามจากการโจมตีระบบโดยผู้ไม่ประสงค์ดี ที่อาจส่งผลให้ข้อมูลสารสนเทศ และการสื่อสาร

11.1.4 ด้านขีดจำกัดในการให้บริการของระบบสารสนเทศ ที่อาจส่งผลให้ไม่สามารถใช้งานหรือให้บริการได้

11.1.5 ด้านกายภาพ หรือภัยธรรมชาติ

11.1.6 หรือด้านอื่นๆ ที่อาจเกิดขึ้นได้

11.2 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องกำหนดขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ของแผนกฯ พร้อมทั้งกำหนดหน้าที่และผู้รับผิดชอบที่ชัดเจน

11.3 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องบันทึกเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และค่าใช้จ่ายที่เกิดจากการเสียหาย เพื่อเรียนรู้และป้องกันไม่ให้เกิดซ้ำขึ้นอีก

11.4 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ต้องเก็บรวบรวมหลักฐานสำหรับอ้างอิง ในกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

12. การบริหารความต่อเนื่องในการดำเนินงานของแผนกฯ

12.1 แผนกฯต้องมีระเบียบปฏิบัติในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งมีแผนฉุกเฉินในการกู้คืนระบบกรณีที่ระบบเกิดความเสียหาย

12.2 หัวหน้างานบริการระบบเครือข่ายคอมพิวเตอร์ต้องมีการทดสอบและปรับปรุงแผนฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

13. ด้านการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ

13.1 แผนกฯ ต้องระบุข้อกำหนดทางกฎหมาย และนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์เป็นลายลักษณ์อักษรชัดเจน และมีการปรับปรุงให้ทันสมัยทุกปี

13.2 แผนกฯ ต้องควบคุมให้ผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ทุกคนปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ นโยบายการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ และไม่ละเมิดข้อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

13.3 แผนกฯ ต้องมีแผนการตรวจประเมินความปลอดภัยของระบบสารสนเทศของแผนกฯ โดยผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของแผนกฯเอง หรือโดยบุคคลภายนอก และต้องมีการควบคุมเครื่องมือหรือซอฟท์แวร์ที่ใช้ในการตรวจประเมิน เพื่อป้องกันการใช้งานผิดวัตถุประสงค์หรือการเปิดเผยข้อมูลตรวจประเมินโดยไม่ได้รับอนุญาต

14. ข้อตกลงในการให้บริการระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ (Service Agreement)

14.1 บริการชื่อผู้ใช้งานและรหัสผ่านส่วนตัวสำหรับการเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศ SiS

14.1.1 เมื่อผู้ใช้งานเป็นพนักงานใหม่จะต้องผ่านขั้นตอนการขอบัญชีผู้ใช้งาน การรับทราบนโยบายการใช้งานและรับทราบสัญญารักษาความลับ ของบริษัทฯ

14.1.2 ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านของตนเองทันที หลังจากได้รับรหัสผ่านจากผู้ดูแลระบบ โดยการตั้งรหัสผ่านใหม่ ตามข้อตกลงในหัวข้อ 15

14.1.3 บริษัทฯ มีมาตรการป้องกันการป้อนรหัสผ่านผิดพลาดซ้ำหลายครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต และรักษาความปลอดภัยของบัญชีผู้ใช้งาน โดยมีรายละเอียดดังต่อไปนี้

14.1.3.1 สำหรับระบบ SAP

- หากผู้ใช้งานใส่รหัสผิด 3 ครั้ง ระบบจะปิดหน้าจอการทำงาน
- หากใส่รหัสผิด 6 ครั้งต่อเนื่อง ระบบจะทำการล็อค SAP User
- หาก SAP User ถูกล็อคการใช้งาน ผู้ใช้งานปลดล็อคได้เองผ่าน Unlock user DB ใน Lotus Notes สำหรับพนักงานที่ไม่มี Lotus Notes User ให้หัวหน้าเป็นผู้ดำเนินการปลดล็อคแทน
- หากปลดล็อคครบ 1 ครั้งต่อวัน แล้วยังไม่สามารถเข้าใช้งานได้ ผู้ใช้งานต้องติดต่อแผนกฯ เพื่อปลดล็อคบัญชีและขอสร้างรหัสผ่านใหม่

14.1.4 ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านการเข้าถึงระบบ SAP ของตนเองอย่างน้อยทุกๆ 90 วัน โดยการตั้งรหัสผ่านใหม่ ตามข้อตกลงในหัวข้อ 15

14.1.5 ผู้ใช้งานต้องรับผิดชอบในการจัดเก็บและรักษารหัสผ่านของตนเองให้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้หากมีผู้อื่นล่วงรู้ข้อมูลอันเป็นความลับนี้ และนำไปใช้งานในทางที่ผิด ยกเว้นกรณีที่สอบสวนโดยตัวแทนของบริษัทฯหรือเจ้าพนักงานแล้วพบว่าไม่ใช่ความผิดของผู้ใช้งานคนนั้นๆ

14.1.6 ระบบจะทำการออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานระบบเป็นเวลา 3,900 วินาที (65 นาที) และจะปิดหน้าจอการทำงานนั้นทันที

14.2 การเชื่อมต่อผ่านสายเข้าสู่ระบบเครือข่าย SiS

14.2.1 การเชื่อมต่อผ่านสายเข้าสู่ระบบเครือข่าย SiS จะต้องตั้งค่า Proxy ตามที่บริษัทฯ กำหนดจึงจะสามารถใช้งานระบบเครือข่ายได้

14.2.2 ผู้ใช้งานต้องมีบัญชีผู้ใช้งานระบบเครือข่ายของบริษัทฯ เพื่อใช้ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่าย SiS

14.3 การเชื่อมต่อแบบไร้สายเข้าสู่ระบบเครือข่าย SiS

14.3.1 ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายของบริษัทฯ จึงจะสามารถใช้งานระบบเครือข่ายไร้สายนี้ได้

14.3.2 ระบบเครือข่ายไร้สายของบริษัทฯ จะใช้ชื่อว่า **“SIS”** ซึ่งต้องระบุตัวตนก่อนเข้าใช้งาน

14.3.3 ผู้ใช้งานระบบเครือข่ายไร้สาย ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯอย่างเคร่งครัด

14.4 บริการสืบค้นข้อมูลผ่านระบบเครือข่าย Internet และ Intranet

14.4.1 ผู้ใช้งานสืบค้นข้อมูลผ่านระบบเครือข่าย Internet และ Intranet จะต้องระบุตัวตนก่อนเข้าใช้งานทุกครั้ง

14.4.2 ผู้ใช้งานต้องระมัดระวังในการใช้งาน หลีกเลี่ยงการเข้าสืบค้นข้อมูลในแหล่งที่ไม่ปลอดภัย

14.4.3 ผู้ใช้งานต้องปฏิบัติตามคำแนะนำในคู่มือการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

14.4.4 ผู้ใช้งานต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

14.4.5 ผู้ใช้งานต้องไม่ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่างเด็ดขาด

14.5 บริการสืบค้นข้อมูลผ่านระบบฐานข้อมูลออนไลน์

14.5.1 การใช้งานระบบฐานข้อมูลออนไลน์ของบริษัทฯนั้น ผู้ใช้งานจะต้องเชื่อมต่อระบบอินเทอร์เน็ตด้วยจึงจะสามารถใช้งานได้

14.5.2 ในกรณีที่ผู้ให้บริการอินเทอร์เน็ตของบริษัทฯไม่สามารถให้บริการได้ อาจจะส่งผลกระทบให้ไม่สามารถใช้งานระบบฐานข้อมูลออนไลน์ด้วย

14.6 บริการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับพนักงาน

14.6.1 บริษัทฯ เป็นผู้สร้างและอำนวยความสะดวกในการใช้งานจดหมายอิเล็กทรอนิกส์ผ่าน Microsoft 365 เพื่อใช้งานสนับสนุนการดำเนินงานของบริษัทฯ

14.6.2 ผู้ใช้งานต้องปฏิบัติตามข้อกฎหมาย และไม่ใช้งานในลักษณะที่ก่อให้เกิดความเสียหายกับผู้อื่น หรือบริษัทฯ โดยผู้ใช้งานต้องรับผิดชอบในการใช้งานทั้งหมด ยกเว้นผู้ใช้งานพิสูจน์ได้ว่าตนมิใช้ผู้กระทำ

14.6.3 ผู้ใช้งานต้องไม่ใช้งานบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ร่วมกับผู้อื่น หรือแจกจ่ายบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ไปให้กับผู้อื่น

14.6.4 กล่องจดหมายที่ผู้ใช้งานได้รับหลังจากได้รับบัญชีผู้ใช้งานเรียบร้อยแล้วจะมีขนาดขั้นต่ำ 50 GB และในการส่งจดหมายพร้อมแต่ละครั้งต้องมีขนาดไม่เกิน 35 MB

14.6.5 แผนกฯ อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้บริการ เพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิ์หรือทรัพย์สินของบริษัทฯ หรือของผู้ใช้บริการอื่น

14.6.6 แผนกฯ อาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบการให้บริการ

14.6.7 บริษัทฯ จะไม่รับประกันความเสียหายหรือสูญหายของข้อมูลที่เก็บไว้ในระบบ

14.6.8 แผนกฯ สงวนสิทธิ์ในเปลี่ยนแปลงบริการหรือตัดทอนลักษณะใดของบริการ ไม่ว่าเหตุผลใดก็ตามได้ตลอดเวลา และอาจยกเลิกหรือระงับการบริการผู้ใช้บริการเมื่อพบว่าละเมิดข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์ของบริษัทฯ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

14.6.9 ข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์นี้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ดังนั้นผู้ให้บริการมีสิทธิ์ในการส่งข้อมูลการให้บริการเพิ่มเติมให้กับผู้ใช้บริการ ผ่านทางจดหมายอิเล็กทรอนิกส์หรือทางหน้าเว็บไซต์บริการจดหมายอิเล็กทรอนิกส์ของบริษัทฯ

14.7 บริการดาวน์โหลดซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้อง ฟรีซอฟท์แวร์ หรือซอฟท์แวร์แบบเปิดเผยรหัสที่มีให้บริการในระบบเครือข่าย SiS

14.7.1 บริการนี้จัดทำขึ้นเพื่ออำนวยความสะดวกให้กับประชาคม บริษัทฯ ได้ใช้ซอฟท์แวร์ลิขสิทธิ์ที่ถูกต้องตามกฎหมาย ประกอบกับรัฐบาลได้กำหนดมาตรการป้องกันการละเมิดลิขสิทธิ์ซอฟท์แวร์ โดยขอความร่วมมือกับส่วนราชการต่างๆ ให้ดำเนินการจัดหาซอฟท์แวร์ถูกกฎหมายมาใช้งานต่อไป

14.7.2 สามารถใช้งานซอฟท์แวร์ลิขสิทธิ์ได้เฉพาะเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของบริษัทฯ เท่านั้น

14.7.3 หากผู้ใช้งานนำซอฟท์แวร์ลิขสิทธิ์ไปใช้งานกับเครื่องคอมพิวเตอร์ส่วนบุคคล บริษัทฯจะไม่รับผิดชอบผลจากการกระทำดังกล่าวใดๆทั้งสิ้น

14.7.4 ซอฟท์แวร์เหล่านี้จะให้บริการดาวน์โหลดผ่านระบบเครือข่าย SiS เท่านั้น ไม่มีบริการทำซ้ำหรือคัดลอกลงบนสื่อบันทึกข้อมูลเพื่อแจกจ่ายใดๆทั้งสิ้น

14.8 บริการฝากเครื่องคอมพิวเตอร์แม่ข่ายสำหรับหน่วยงานในสังกัดบริษัทฯ

14.8.1 หน่วยงานเจ้าของเครื่องคอมพิวเตอร์แม่ข่ายต้องยอมรับ และปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

14.8.2 เครื่องคอมพิวเตอร์แม่ข่ายที่นำมาฝากต้องผ่านการตรวจสอบจากผู้ดูแลระบบเครือข่ายเพื่อให้มั่นใจว่าจะไม่รบกวนการทำงานของระบบอื่นๆ และไม่เป็นช่องโหว่ต่อการจู่โจม โดยหากตรวจสอบแล้วพบความเสี่ยงที่อาจจะเป็นอันตรายต่อระบบอื่นๆ จะไม่อนุญาตให้นำมาฝากไว้ในห้องควบคุมระบบเครือข่ายได้จนกว่าจะได้รับการแก้ไขโดยหน่วยงานเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย

14.8.3 หากเครื่องคอมพิวเตอร์แม่ข่ายที่นำมาฝากเป็นสาเหตุที่ทำให้ระบบอื่นๆทำงานผิดปกติ หรือไม่สามารถให้บริการได้ ผู้ดูแลระบบเครือข่ายจะสงวนสิทธิ์ในการยกเลิกการการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวออกจากระบบเครือข่ายทันที โดยไม่จำเป็นต้องแจ้งล่วงหน้า เพื่อคงไว้ซึ่งมาตรการด้านความปลอดภัย

14.9 การขอใช้บริการพิเศษอื่นๆที่จำเป็นต้องเปิด Port Firewall ของบริษัทฯ สำหรับพนักงานในสังกัดบริษัทฯ

14.9.1 บุคลากรผู้ขอต้องยอมรับ และปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

14.9.2 วัตถุประสงค์ในการใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่างๆของบริษัทฯ และต้องไม่ขัดต่อกฎหมาย

14.9.3 บุคลากรผู้ขอต้องทำการขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการฝ่ายปฏิบัติการในการขอแต่ละครั้ง โดยต้องระบุข้อมูลทางเทคนิคโดยละเอียดดังต่อไปนี้

14.9.3.1 หมายเลข Port ที่ต้องการขอให้เปิด

14.9.3.2 หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสารด้วย

14.9.3.3 วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้ผ่าน Port นั้นๆ

14.9.3.4 วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

14.9.4 ทางแผนกฯ จะไม่อนุมัติให้ใช้งาน หากทำการพิจารณาแล้วพบว่าการขอใช้งานขัดต่อนโยบาย ประกาศ ระเบียบ ของบริษัทฯ หรือขัดต่อกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ

14.9.5 ภายหลังการอนุมัติให้ใช้งานแล้วพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบข้องบริษัท หรือขัดต่อกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัทฯ ทางแผนกฯจะยกเลิกการให้บริการทันที

15. ข้อตกลงการควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) สำหรับใช้งานระบบสารสนเทศ

15.1 สำหรับการเข้าถึงระบบ SAP ต้องมีระบบตรวจสอบตัวตนและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศ รวมถึงข้อมูลสำคัญและข้อมูลส่วนบุคคล ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น ให้ใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม

- ควรกำหนดให้รหัสผ่านมีความยาวไม่น้อยกว่า 8 ตัวอักษร
- รหัสผ่านควรประกอบไปด้วย 3 ใน 4 อย่างต่อไปนี้ อักขระพิเศษ, ตัวเลข, ตัวอักษรใหญ่และตัวอักษรเล็ก
- ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 90 วัน
- ระบบสารสนเทศจะทำการล็อคหรือปิดกั้นบัญชีผู้ใช้งานชั่วคราวเมื่อใส่รหัสผิด 6 ครั้งต่อเนื่อง
- สำหรับระบบที่มีการเปิดให้ผู้ใช้งานเข้าใช้งานผ่านอินเตอร์เน็ตได้ ควรเพิ่มการยืนยันตัวตนหลายปัจจัย (MFA)
- ส่วนงานพัฒนาระบบสารสนเทศมีหน้าที่ในการทบทวนสิทธิ์การเข้าใช้ระบบ SAP เป็นประจำทุกปี
- การแก้ไขหรือทำลาย User ID
    - กรณี ลาออก/พ้นสภาพการเป็นพนักงาน ให้ทำการปิดการใช้งาน/ลบ User ID ภายใน 3 วันหลังประกาศฯ มีผล
    - กรณี ย้ายหน่วยงานโดยหน่วยงานใหม่ไม่มีความจำเป็นต้องใช้งาน ให้ทำการลบ User ID ภายใน 3 วันหลังประกาศฯมีผล

15.2 กรณีที่ระบบสารสนเทศใดไม่สามารถกำหนดรหัสผ่าน (Password Policy) ได้ตามข้อกำหนด เนื่องจากข้อจำกัดทางเทคโนโลยี ต้องทำการควบคุมการเข้าถึงระบบสารสนเทศโดยอนุญาตให้เข้าถึงได้ผ่านทางระบบเครือข่ายภายใน (Intranet) เท่านั้น

15.3 ผู้ใช้งานทุกคนต้องรับผิดชอบในการเก็บรักษาบัญชีผู้ใช้งานและรหัสผ่านของตนเอง โดยห้ามเปิดเผย แบ่งปัน หรืออนุญาตให้บุคคลอื่นใช้บัญชีผู้ใช้งานหรือรหัสผ่านของตน เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยมิชอบ และลดความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล

<u>แนวทางการรักษาความปลอดภัยระบบสารสนเทศ</u>

1. ให้ผู้บริหารและพนักงานทุกคน ตระหนักถึงนโยบายความปลอดภัยสารสนเทศของบริษัทฯ รวมทั้งปฏิบัติตามอย่างเคร่งครัด
2. ให้ผู้บริหารและพนักงานทุกคน ปฏิบัติตนตามแนวทางในข้อตกลงในการให้บริการระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ
3. หากมีการใช้งานสารสนเทศที่ขัดต่อนโยบาย ประกาศ และระเบียบข้องบริษัท หรือขัดต่อกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัท ทางแผนกฯ สามารถยกเลิกการใช้บริการได้ทันที

นโยบายความปลอดภัยระบบสารสนเทศนี้ ได้รับการอนุมัติโดยคณะกรรมการบริษัท ในการประชุมคณะกรรมการบริษัท ครั้งที่ 6/2568 เมื่อวันที่ 12 ธันวาคม 2568

นโยบายนี้ให้มีผลบังคับใช้ นับตั้งแต่วันที่ 1 มกราคม 2569 เป็นต้นไป

นางวรีพร สิทธิชัยศรีชาติ
ผู้อำนวยการฝ่ายปฏิบัติการ
บริษัท เอสไอเอส ดิสทริบิวชั่น (ประเทศไทย) จำกัด (มหาชน)