บริษัท เอจีอี เทอร์มินอล จำกัด และบริษัทในเครือ	เอกสารหมายเลข : AGET-ST-IT แก้ไขครั้งที่ : 00 วันที่อนุมัติใช้ : 2 มกราคม 2568
นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ	

บริษัท เอจีอี เทอร์มินอล จำกัด
นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

ผู้จัดทำ นายธานินทร์ อมรสถิตย์วงศ์ ผู้จัดการฝ่ายสารสนเทศ	Tanin A.	**วันที่** : 2 มกราคม 2568
ผู้ทบทวน นายอธิภัทร ควรสถาพร กรรมการผู้จัดการ/ผู้ช่วยกรรมการผู้จัดการ		**วันที่** : 2 มกราคม 2568
ผู้อนุมัติ นายพนม ควรสถาพร ประธานกรรมการบริษัท		**วันที่** : 2 มกราคม 2568

นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

เพื่อให้การใช้งาน การให้บริการ การดำเนินงาน และการเก็บรักษาข้อมูลด้านระบบเทคโนโลยีสารสนเทศของบริษัท เอจีอี เทอร์มินอล กำจัด มหาชน มีความมั่นคง ปลอดภัย และสามารถตอบสนองการใช้งานได้อย่างมีมั่นคงและประสิทธิภาพจึงกำหนดวิธีปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

ข้อ 1 การรักษาความมั่นคงปลอดภัยด้านพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ (Data Center)

1.1 ข้อกำหนดทั่วไปของการรักษาความปลอดภัยพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ

1.1.1 ต้องติดป้ายแสดงเขตพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศให้ชัดเจน

1.1.2 ดำเนินการสร้างสภาพแวดล้อมในการปฏิบัติการระบบคอมพิวเตอร์ที่ดี เหมาะสม และปลอดภัย

1.1.3 ห้ามสูบบุหรี่และนำอาหาร เครื่องดื่ม เข้ามาภายในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ โดยเด็ดขาด

1.1.4 ห้ามนำและเก็บรักษาน้ำมันเชื้อเพลิงและวัสดุไวไฟ ในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ โดยเด็ดขาด

1.1.5 ให้แยกวัสดุที่อาจเกิดการสันดาปและลุกไหม้ออกจากกันและทำเครื่องหมายหรือสัญลักษณ์แสดงโดยชัดเจน

1.1.6 ห้ามเก็บสิ่งของหรือสัมภาระที่ไม่เกี่ยวข้องกับการปฏิบัติงานในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ หรือบริเวณอื่นใดซึ่งมิได้เป็นสถานที่ที่จัดเตรียมไว้

1.1.7 ให้ดำเนินการกำกับ ควบคุม ดูแล รักษาความสะอาด บำรุงรักษาและบริหารการใช้พื้นที่ปฏิบัติการสารสนเทศ ให้เป็นไปโดยเรียบร้อย สะอาด ปลอดภัย ประหยัด และเหมาะสมต่อลักษณะการทำงาน เพื่อให้การทำงานสามารถดำเนินการได้อย่างต่อเนื่อง

1.1.8 จัดให้มีการดูแล บำรุงรักษาและตรวจสอบสภาพของการทำงานการใช้งานของการทำงาน การใช้งานของระบบ คอมพิวเตอร์และอุปกรณ์ต่อร่วมต่างๆ อย่างสม่ำเสมอต่อเนื่อง ให้อยู่ในสภาพที่สะอาดปลอดภัย และเป็นไปตามมาตรฐานหรือคุณสมบัติของอุปกรณ์แต่ละระบบตามระยะเวลาและขั้นตอนที่อุปกรณ์แต่ละประเภทกำหนดหรือตามแผนการบำรุงรักษาระบบคอมพิวเตอร์นั้นๆ

1.1.9 พื้นที่เก็บอุปกรณ์บันทึกข้อมูล สิ่งพิมพ์ที่ใช้สำรองข้อมูล (Backup) ระบบสารสนเทศ รวมถึงกระบวนการปฏิบัติงาน (Process) เพื่อกู้คืนระบบสารสนเทศจะต้องแยกออกไม่ติดตั้งหรือจัดเก็บภายในอาคารเดียวกันกับสถานที่ติดตั้งระบบคอมพิวเตอร์

1.1.10 จัดให้มีการดำเนินการในส่วนที่เกี่ยวข้องกับการป้องกันการรั่วไหลของข้อมูล การลักลอบหรือขโมยข้อมูล การทำลายข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบคอมพิวเตอร์

1.1.12 จัดให้มีการควบคุม ดูแล การใช้อุปกรณ์สื่อสัญญาณทุกชนิดอย่างเหมาะสม เพื่อป้องกันการรบกวน หรือทำความสูญเสียหรือเสียหายแก่ระบบสารสนเทศ

1.1.13 จัดให้มีการดำเนินการในส่วนที่เกี่ยวข้องกับการควบคุมและป้องกันบุคคลภายนอก หรือผู้ที่มิได้เกี่ยวข้องเข้า – ออก พื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ

1.1.14 ส่วนงานเจ้าของพื้นที่ต้องจัดให้มีแผนป้องกันภัยยามฉุกเฉินภายในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ และดำเนินการซักซ้อมอย่างน้อยปีละ 1 ครั้ง รวมทั้งจัดให้มีการทบทวนแผนป้องกันภัยฉุกเฉินอย่างสม่ำเสมอ

1.1.15 ผู้ปฏิบัติงานที่ไม่ได้ปฏิบัติงานในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ บุคคลภายนอกและหรือพนักงานของบริษัทคู่สัญญามีความประสงค์จะเข้ามาปฏิบัติงานในพื้นที่ศูนย์ปฏิบัติการระบบสารสนเทศ จะต้อง

ได้รับอนุญาตจากผู้จัดการแผนกสังกัดฝ่าย IT (ขึ้นไป) และให้อยู่ในความดูแลโดยใกล้ชิดจากเจ้าหน้าที่ผู้ที่เกี่ยวข้องในพื้นที่ทั้งในและนอกเวลาทำการจนกว่าการปฏิบัติงานจะแล้วเสร็จ

1.1.16 บุคคลภายนอกและพนักงานของบริษัทคู่สัญญาที่ได้รับอนุญาตจากผู้จัดการแผนกสังกัดฝ่าย IT (ขึ้นไป) ให้เข้ามาปฏิบัติงานในพื้นที่ปฏิบัติการสารสนเทศ จะต้องปฏิบัติตามกฎเกณฑ์ต่างๆ ของบริษัทโดยเคร่งครัดทุกกรณี

ข้อ 2 การรักษาความมั่นคงปลอดภัยด้านเครื่องคอมพิวเตอร์

2.1 ผู้ดูแลเครื่องคอมพิวเตอร์ มีหน้าที่ดูแล บำรุงรักษาเครื่องคอมพิวเตอร์ ในเบื้องต้นสามารถใช้งานได้ดีอยู่เสมอ และอยู่ในสภาพที่เรียบร้อยสมบูรณ์

2.2 ผู้บริหารเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องคอมพิวเตอร์แม่ข่าย จะต้องรักษามารยาท จรรยาบรรณ และความลับของข้อมูลซึ่งเป็นขององค์กรและผู้อื่น

2.3 ให้ผู้ดูแลเครื่องคอมพิวเตอร์ ตรวจสอบสภาพแวดล้อมในสถานที่ทำงานให้เหมาะสมกับเครื่องคอมพิวเตอร์ อย่างน้อยดังนี้

2.3.1 ในกรณีที่ใช้งานมีปัญหาเรื่องกระแสไฟฟ้า ให้จัดเตรียม UPS ไว้ใช้งาน

2.3.2 หลีกเลี่ยงการติดตั้งคอมพิวเตอร์ หรือสื่อคอมพิวเตอร์ต่างๆ ในสถานที่ ดังนี้

2.3.2.1 สถานที่ที่มีอุณหภูมิสูงหรือใกล้แหล่งกำเนิดความร้อนหรือเครื่องคอมพิวเตอร์สัมผัสแสงแดดโดยตรง

2.3.2.2 สถานที่ที่มีฝุ่นละอองมาก

2.3.2.3 สถานที่ที่มีความชื้นสูง

2.3.2.4 สถานที่ที่มีสนามแม่เหล็กรบกวน เช่น ใกล้หม้อแปลงไฟฟ้า

2.4 ผู้บริหารเครื่องคอมพิวเตอร์แม่ข่ายและผู้ใช้งานเครื่องคอมพิวเตอร์ ต้องจัดให้มีระบบสำรองข้อมูลลงในสื่อคอมพิวเตอร์ชนิดต่างๆ ตามความจำเป็น เช่น Floppy Disk, CD, Tape Backup, Hard Disk Backup หรืออื่นๆ

2.5 ให้ผู้ดูแลเครื่องคอมพิวเตอร์ติดตั้งโปรแกรมหรืออุปกรณ์ป้องกันไวรัสคอมพิวเตอร์ทุกเครื่องติดตามข่าวเกี่ยวกับไวรัสคอมพิวเตอร์ และปรับปรุงข้อมูลในโปรกแกรมป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัยอยู่เสมอ

2.6 ข้อปฏิบัติของส่วนงานในการรักษาความปลอดภัยด้านเครื่องคอมพิวเตอร์

2.6.1 ระมัดระวังการติด Virus Computer โดยให้ปฏิบัติตามการรักษาความปลอดภัยด้านการป้องกันไวรัสคอมพิวเตอร์

2.6.2 ห้ามการติดตั้งโปรแกรม เกมส์ เพลง ภาพยนต์ที่ไม่เกี่ยวข้องกับการทำงานและ(หรือ)ไม่มีลิขสิทธิ์ รวมไปถึงอุปกรณ์ต่อพ่วงบางชนิดและ(หรือ)อุปกรณ์ใดๆ ที่เป็นการรบกวนระบบเครือข่ายสารสนเทศ โดยไม่ได้รับอนุญาต

2.6.3 ไม่เปิดระบบงาน หรืองานใดๆ ไว้ในเครื่องคอมพิวเตอร์ในขณะที่ไม่อยู่หน้าจอภาพ เนื่องจากข้อมูลต่างๆ อาจจะสูญหาย เสียหาหรือรั่วไหลได้

2.6.4 การปิดเครื่องคอมพิวเตอร์ต้องปิดตามขั้นตอนการปิดเครื่องคอมพิวเตอร์ที่ถูกต้อง เช่น ปิดโปรแกรมต่างๆ ที่เปิดไว้ทั้งหมดและปิดเครื่องคอมพิวเตอร์โดยคำสั่ง Shut down เป็นต้น

ข้อ 3 การรักษาความปลอดภัยด้านเครือข่ายคอมพิวเตอร์

3.1 ผู้ใช้งานเครือข่าย ต้องไม่ปฏิบัติการใดๆ ที่เกี่ยวข้องกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน

3.2 ห้ามมิให้ผู้ใช้งานเครือข่ายคอมพิวเตอร์กระทำการใดๆ ที่เกี่ยวกับการประกอบธุรกิจ หรือประโยชน์อื่นใดในเชิงธุรกิจอันมิใช่กิจการและธุรกรรมของบริษัทผ่านเครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ของบริษัท

3.3 ผู้ใช้งานเครือข่ายคอมพิวเตอร์จะต้องไม่ละเมิดต่อผู้อื่น เช่น ไม่บุกรุกเข้าสู่บัญชีผู้ใช้งานของผู้อื่น ไม่อ่าน เขียน ลบ เปลี่ยนแปลง ทำสำเนาและหรือแก้ไขใดๆ ในข้อมูลส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เป็นต้น

3.4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรักษามารยาท จรรยาบรรณ และการรักษาความลับของข้อมูลซึ่งเป็นขององค์กรและผู้อื่น

3.5 ผู้ใช้งานเครือข่ายคอมพิวเตอร์ต้องไม่ทำการเผยแพร่ข่าวสารใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพ หรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายซึ่งถือว่าเป็นการละเมิดต่อผู้อื่นและ(หรือ)ขัดต่อกฎหมาย

3.6 ส่วนงานใดที่มีความต้องการจัดทำระบบงานซึ่งจำเป็นต้องใช้การเชื่อมต่อผ่านเครือข่ายคอมพิวเตอร์ ต้องแจ้งให้ผู้ดูแลเครือข่ายคอมพิวเตอร์ทราบตั้งแต่ขั้นตอนของการวางแผนจัดทำโครงการเพื่อการเตรียมการรองรับการเชื่อมต่อทางด้านเครือข่ายคอมพิวเตอร์ของระบบงานนั้นๆ

3.7 การขออนุญาตใช้งานเครือข่ายย่อย หมายเลขไอพี (IP Address) ต้องขอใช้ผ่านส่วนงานต้นสังกัดมายังผู้ดูแลเครือข่ายคอมพิวเตอร์เพื่อพิจารณาดำเนินการเป็นลายลักษณ์อักษร

3.8 ส่วนงานที่มีและหรือจัดให้มีการเชื่อมต่อจากระยะไกลผ่านทางอุปกรณ์ Network หรือผ่านโปรแกรม Remote Access เพื่อการเชื่อมต่อผ่านคู่สายโทรศัพท์ สายสัญญาณเครือข่ายจากผู้ให้บริการภายนอก หรือ Internet ต้องแจ้งให้ผู้ดูแลเครือข่ายคอมพิวเตอร์ทราบเป็นลายลักษณ์อักษร และต้องควบคุม ดูแลรักษาความปลอดภัยของระบบไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปใช้งานและไม่ให้มีการนำไปใช้ในการประกอบธุรกิจ หรือประโยชน์อื่นใดในเชิงธุรกิจ อันมิใช่กิจการและธุรกรรมของบริษัท

3.9 ส่วนงานที่ใช้ระบบเครือข่ายไร้สาย (Wireless LAN) ต้องจัดให้มีการควบคุมการเชื่อมต่ออย่างเข้มงวด โดยต้องควบคุมดูแลรักษาความปลอดภัยของระบบไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปใช้งาน และไม่ให้มีการนำไปใช้ในการประกอบธุรกิจหรือประโยชน์อื่นใดในเชิงธุรกิจอันมิใช่กิจการและธุรกรรมของบริษัท

3.10 ห้ามผู้ไม่มีหน้าที่เกี่ยวข้องกับการดูแลเครือข่ายคอมพิวเตอร์ใช้โปรแกรมที่สามารถจัดดูข้อมูลภายในเครือข่ายคอมพิวเตอร์ เพื่อดูข้อมูลที่รับ – ส่งผ่านในเครือข่ายคอมพิวเตอร์

ข้อ 4 การรักษาความปลอดภัยด้านข้อมูลสารสนเทศ

4.1 การรับ – ส่ง ข้อมูลสารสนเทศไม่ว่าในสื่อหรือวิธีการใดที่มีความสำคัญ ระหว่างส่วนงานทั้งส่วนงานภายในและภายนอก จะต้องได้รับอนุญาตจากผู้บังคับบัญชาที่ดูแลระบบสารสนเทศนั้นๆ โดยมีการจัดทำทะเบียนควบคุมการรับส่งข้อมูลสารสนเทศนั้นๆ ไว้อย่างชัดเจน

4.2 กรณีที่มีความจำเป็นต้องส่งผ่านข้อมูลสารสนเทศจากระบบ ERP หรือ ระบบที่มีความสำคัญออกไปในระบบอินเทอร์เน็ตหรืออินทราเน็ต ให้มีการเข้ารหัสของข้อมูลสารสนเทศที่จัดส่งออกไป

4.3 การแบ่งปัน (Share) ข้อมูลให้แบ่งปันเฉพาะสิ่งที่ต้องการ และต้องกำหนดรหัสผ่านหรือกำหนดการเข้าถึงให้เฉพาะบุคคลหรือหน่วยงานที่เกี่ยวข้องเท่านั้น ทุกครั้ง และเมื่อหมดความจำเป็นในการแบ่งปันนั้นให้ยกเลิกการแบ่งปันทันที

ข้อ 5 การรักษาความปลอดภัยด้านซอฟท์แวร์

5.1 ให้ส่วนงานจัดเก็บเอกสารแสดงลิขสิทธิ์และซอฟท์แวร์ต้นฉบับอย่างดีที่สุด เว้นแต่ลิขสิทธิ์รวม ให้อยู่ในความรับผิดชอบของฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

5.2 กรณีเข้าใช้ระบบงาน เมื่อไม่มีการทำงานใดๆ กับระบบในช่วงระยะเวลาหนึ่ง ให้ระบบทำการตัดการเชื่อมต่อเข้าสู่ระบบ

5.3 ให้ส่วนงานจัดให้มีการบำรุงรักษาซอฟท์แวร์ให้สามารถใช้งานได้อย่างต่อเนื่อง

5.4 ซอฟท์แวร์สำหรับเครื่องผู้บริหาร ให้ส่วนงานรับผิดชอบดูแลเครื่องนั้นๆ เป็นผู้ดูแลและเก็บรักษาลิขสิทธิ์ซอฟท์แวร์

ข้อ 6 การรักษาความปลอดภัยด้านการสำรองและการกู้คืนสภาพระบบสารสนเทศ

6.1 ส่วนงานที่รับผิดชอบระบบสารสนเทศจะต้องจัดทำแผนการดำเนินการสำรองระบบสารสนเทศ ซึ่งได้รับความเป็นชอบจากหัวหน้าส่วนงานที่รับผิดชอบระบบงานสารสนเทศนั้นๆ โดยมีแนวทางปฏิบัติในการสำรองระบบสารสนเทศ ต้องมีรายละเอียดของหัวข้ออย่างน้อยดังต่อไปนี้

6.1.1 ลำดับความสำคัญของระบบงานหรือระบบสารสนเทศที่จะทำสำรอง

6.1.2 ประเภทของสื่อบันทึกข้อมูลที่ใช้ในการสำรองระบบสารสนเทศ

6.1.3 ตารางเวลาและความถี่ในการสำรองของแต่ละระบบงาน

6.1.4 ระยะเวลาและจำนวนชุดที่ต้องการจัดเก็บของสื่อบันทึกข้อมูล รวมถึงการนำสื่อบันทึกข้อมูลกลับมาใช้ใหม่ของแต่ละระบบงาน

6.1.5 ข้อมูลรายละเอียดโครงสร้างของระบบงานและหรือระบบสารสนเทศ ประกอบด้วย

6.1.5.1 แผนภูมิส่วนงานที่เกี่ยวข้อง

6.1.5.2 แผนภูมิแสดงการเคลื่อนไหวของข้อมูลและที่เกี่ยวข้อง

6.1.5.3 รายละเอียดการทำงานของระบบงานและที่เกี่ยวข้อง

6.1.6 ขั้นตอนการทำงานและความรับผิดชอบในด้านต่างๆ

6.1.7 สถานที่หลักและสถานที่รอง สำหรับใช้จัดเก็บสื่อบันทึกข้อมูลที่ใช้ในการสำรองระบบสารสนเทศ

6.1.8 วิธีการควบคุมการใช้งานสื่อบันทึกข้อมูล

6.1.9 จัดทำสมุดบันทึก (Log Book) เพื่อบันทึกการปฏิบัติงานของการสำรองระบบสารสนเทศ โดยมีระยะเวลาการเก็บสมุดบันทึกไม่น้อยกว่า 1 ปี หรือ บันทึก Log ไว้ในระบบฐานข้อมูลของโปรแกรมที่ใช้สำรองข้อมูล

6.1.10 ให้มีการปรับปรุงเอกสารสำรองระบบสารสนเทศทุกๆ 1 ปี หรือเมื่อมีการเปลี่ยนแปลงของระบบสารสนเทศ

6.1.11 ขั้นตอนการตรวจสอบผลการทำสำรองระบบสารสนเทศ

6.1.12 เงื่อนไขและข้อจำกัดต่างๆ ในการทำสำเนาระบบสารสนเทศ

6.2 แนวทางการกู้คืนสภาพระบบสารสนเทศ (Recovery) ต้องครอบคลุมหัวข้อดังต่อไปนี้เป็นอย่างน้อย

6.2.1 ลำดับความสำคัญของระบบงานและหรือระบบสารสนเทศ ที่จะทำการกู้คืนสภาพ

6.2.2 ขั้นตอนการทำงานและความรับผิดชอบในด้านต่างๆ

6.2.3 ขั้นตอนการกู้คืนสภาพระบบสารสนเทศ โดยให้มีรายละเอียดอย่างน้อยดังนี้

6.2.3.1 การกู้คืนสภาพระบบคอมพิวเตอร์

6.2.3.2 การกู้คืนสภาพระบบเครือข่าย

6.2.3.3 การกู้คืนสภาพระบบงาน

6.2.3.4 การตรวจสอบการกู้คืนสภาพ

6.2.4 จัดทำบัญชีรายชื่อผู้รับผิดชอบทั้งในและนอกบริษัท รวมทั้งช่องทางการสื่อสารที่สามารถติดต่อได้โดยสะดวก

6.2.5 ให้มีการทดสอบการกู้คืนสภาพระบบสารสนเทศในแต่ละระบบงานอย่างน้อยทุกๆ 12 เดือน พร้อมบันทึกผลการดำเนินงาน และรายงานให้หัวหน้าส่วนงานที่รับผิดชอบทราบ

ข้อ 7 การรักษาความปลอดภัยด้านเอกสารและอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ

7.1 เอกสารและอุปกรณ์บันทึกข้อมูลระบบสารสนเทศที่ไม่ได้มีการใช้งานแล้วให้เก็บไว้ช่วงเวลาหนึ่ง ตามความเหมาะสมและความจำเป็น จากนั้นให้ตรวจสอบให้แน่ใจว่าจะไม่มีการใช้งานอีกต่อไป จำนำเอกสารและอุปกรณ์บันทึกข้อมูลระบบสารสนเทศดังกล่าวไปเก็บไว้ในสถานที่เพื่อรอการทำลายพร้อมทั้งจัดทำป้ายบอกไว้ให้ชัดเจน เช่น วันที่เลิกใช้งาน ชื่อหน่วยงาน ชื่อผู้รับผิดชอบก่อนขออนุมัติต่อ ผู้บังคับบัญชาเพื่อดำเนินการทำลายต่อไป

7.2 การทำลายเอกสารระบบสารสนเทศที่เป็นความลับจะต้องดำเนินการทำลายเอกสารนั้นๆ ด้วยเครื่องทำลายเอกสารเสียก่อนมิให้สามารถใช้งานได้ต่อไป

7.3 การทำลายข้อมูลสารสนเทศที่เก็บอยู่ในสื่อคอมพิวเตอร์ ให้ใช้วิธีการที่มั่นใจได้ว่าข้อมูลได้ถูกลบทิ้งโดยไม่สามารถกู้คืนได้อีก

7.4 การพิมพ์เอกสารระบบสารสนเทศที่เป็นความลับ ให้คำนึงถึงความปลอดภัยของเอกสารที่ถูกพิมพ์

7.5 ให้มีระบบป้องกันการบันทึกในอุปกรณ์บันทึกข้อมูลสารสนเทศที่ยังใช้งานอยู่

7.6 มีการจัดประเภทของอุปกรณ์บันทึกข้อมูลสารสนเทศให้เหมาะสมกับระยะเวลาในการเก็บรักษา

7.7 มีการตรวจสอบความครบถ้วนและสภาพการใช้งานอุปกรณ์บันทึกข้อมูลเป็นระยะๆ

7.8 มีการกำหนดอายุการใช้งานของสื่อบันทึกข้อมูลสารสนเทศ และให้มีการบันทึกวันเริ่มใช้งานและวันสิ้นสุดการใช้งาน

7.9 มาตรฐานการรักษาความปลอดภัยของห้องเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ

7.9.1 การเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ จะต้องจัดทำทะเบียนแสดงรายละเอียดของข้อมูลที่จัดเก็บ

7.9.2 การเก็บอุปกรณ์บันทึกข้อมูลระบบสารสนเทศที่เป็นความลับต้องจัดทำทะเบียนผู้มีสิทธิใช้อุปกรณ์ดังกล่าว

7.9.3 มีการลงทะเบียนทุกครั้งที่มีการยืมหรือคืนอุปกรณ์บันทึกข้อมูลระบบสารสนเทศ

7.9.4 มีการควบคุม ดูแลทางด้านกายภาพของห้องเก็บอุปกรณ์เก็บข้อมูลระบบสารสนเทศเป็นอย่างดี ให้เหมาะกับการเก็บสื่อคอมพิวเตอร์

ข้อ 8 การรักษาความปลอดภัยด้านการใช้รหัสผ่าน

8.1 รหัสผ่าน ให้มีความยาวไม่น้อยกว่า 8 หลัก และเพื่อให้มีความปลอดภัยมากที่สุด รหัสผ่านควรเป็นทั้งชุดของตัวอักษร สัญลักษณ์พิเศษ ตัวเลขคละรวมกัน

8.2 ผู้ปฏิบัติงานที่รับอนุญาตและได้รับสิทธิในการใช้ระบบสารสนเทศ เมื่อได้รับจัดสรร รหัสผ่าน ให้เปลี่ยนรหัสผ่านเป็นของตัวเองที่เหมาะสมและเป็นความลับเฉพาะตัวชุดทันที

8.3 การขอใหม่ เปลี่ยนแปลง ยกเลิก รหัสผ่าน ให้ทำเป็นลายลักษณ์อักษร และในระบบสารสนเทศที่มีความสำคัญ ต้องผ่านความเห็นชอบจากต้นสังกัดก่อนขออนุมัติจากผู้มีอำนาจก่อนจะดำเนินการใดๆ

8.4 ผู้ปฏิบัติงานควรเปลี่ยนแปลงรหัสผ่านของตัวเองใหม่ทุกๆ 90 วัน หรือตามระยะเวลาที่ระบบสารสนเทศนั้นๆ กำหนด

8.5 การเปลี่ยนแปลงรหัสผ่านชุดใหม่ในแต่ละครั้ง จะต้องไม่นำรหัสผ่านชุดเก่ามาใช้ซ้ำอีกเป็นจำนวนสามครั้ง

8.6 เจ้าของรหัสผ่านต้องรับผิดชอบในการปกปิดและรักษารหัสผ่านของตนเองอย่างดีที่สุด โดย

8.6.1 ไม่จดบันทึกรหัสผ่านในที่ที่สามารถพบเห็นได้โดยง่าย

8.6.2 ไม่นำหรือไม่เปิดเผยรหัสผ่านให้บุคคลอื่นรับรู้ หากรหัสผ่านถูกเปิดเผยต้องเปลี่ยนใหม่โดยเร็ว

8.6.3 เมื่อเสร็จสิ้นการใช้งานระบบสารสนเทศแล้ว จะต้องออกจากการใช้ระบบ (Logout) ทุกครั้ง หรือ ทำการ Lock หน้าจอด้วยรหัสผ่าน เมื่อพักการใช้งาน

8.7 หากผู้ปฏิบัติงานพบเห็นหรือสงสัยถึงการล่วงละเมิดต่อความปลอดภัยในการใช้งานหรือประเด็นอื่นใดที่เกิดขึ้นเนื่องจากรหัสผ่านถูกนำไปใช้โดยผู้ที่ไม่ใช่เจ้าของ ต้องรายงานต่อผู้บังคับบัญชาเพื่อแจ้งผู้ดูแลระบบทันที เพื่อทำการตรวจสอบและแก้ไขต่อไป

8.8 มีการจัดการเรื่องความปลอดภัยในส่วนของ Employee Rule Base Management เช่น การใช้สิทธิ์ตามหน้าที่ความรับผิดชอบของพนักงาน เป็นต้น

ข้อ 9 การรักษาความปลอดภัยด้านการป้องกันไวรัสคอมพิวเตอร์

9.1 แนวทางปฏิบัติด้านการป้องกันไวรัสคอมพิวเตอร์

9.1.1 ผู้ดูแลระบบสารสนเทศ

9.1.1.1 ดำเนินการจัดหาโปรแกรมป้องกันไวรัสคอมพิวเตอร์ และอบรมการใช้งานให้กับผู้ดูแลเครื่องคอมพิวเตอร์ของส่วนงานต่างๆ

9.1.1.2 ตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ในระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

9.1.1.3 ตรวจสอบความทันสมัยของโปรแกรมป้องกันไวรัสคอมพิวเตอร์และปรับปรุงให้กับระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ทุกสัปดาห์หรือทันทีที่ได้รับข้อมูลการแพร่กระจายของไวรัสคอมพิวเตอร์ชนิดใหม่

9.1.1.4 แจ้งข้อมูลข่าวสารของไวรัสคอมพิวเตอร์ไปยังผู้ดูแลเครื่องคอมพิวเตอร์และผู้ใช้งานเครื่องคอมพิวเตอร์

9.1.2 ผู้ดูแลเครื่องคอมพิวเตอร์

9.1.2.1 ดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้กับเครื่องคอมพิวเตอร์ทุกเครื่อง โดยประสานงานกับผู้ดูแลระบบสารสนเทศ

9.1.2.2 ตรวจสอบความทันสมัยของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ และปรับปรุงให้กับระบบคอมพิวเตอร์ทุกๆ เครื่องอย่างน้อยสัปดาห์ละ 1 ครั้ง หรือทันทีที่ได้รับข้อมูลการแพร่กระจายของไวรัสคอมพิวเตอร์ชนิดใหม่

9.1.3 ผู้ใช้งานเครื่องคอมพิวเตอร์

9.1.3.1 ผู้ใช้งานเครื่องคอมพิวเตอร์ทุกคนจะต้องมีความรู้ความสามารถในการจัดการข้อมูลและการสำรองข้อมูลด้วยตัวเอง

9.1.3.2 ห้ามนำซอฟท์แวร์หรือข้อมูลที่อาจก่อนให้เกิดความเสียหายต่อระบบสารสนเทศของบริษัทมาติดตั้งใช้งาน

9.1.3.3 ห้ามยกเลิกการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ซึ่งติดตั้งอยู่ในเครื่องคอมพิวเตอร์

9.1.3.4 หากเครื่องคอมพิวเตอร์มีการเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ ให้ปลดสายที่ให้เชื่อมต่อกับเครือข่ายคอมพิวเตอร์ออก เพื่อป้องกันการระบาดของไวรัสคอมพิวเตอร์ผ่านทางเครือข่ายคอมพิวเตอร์

.....

(นายพนม ควรสถาพร)

ประธานกรรมการบริษัท เอจีอี เทอร์มินอล จำกัด

นโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2567 เมื่อวันที่ 27 ธันวาคม 2567 โดยมีผลบังคับใช้ตั้งแต่วันที่ 2 มกราคม 2568 เป็นต้นไป