ประกาศ

บริษัท เจนเนอรัล เอนจิเนียริ่ง จำกัด (มหาชน)

เรื่อง นโยบายบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) แผนกเทคโนโลยีสารสนเทศ เสนอเพื่อพิจารณาเปลี่ยนแปลง นโยบายบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) เพื่อออกเป็นประกาศ โดยมีเนื้อหาดังนี้

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ บริษัท เจนเนอรัล เอนจิเนียริ่ง จำกัด (มหาชน) พ.ศ. 2568

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท เจนเนอรัล เอนจิเนียริ่ง จำกัด (มหาชน) เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงและปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่บริษัท อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายอื่นที่เกี่ยวข้อง บริษัทฯ จึงเห็นสมควรออกประกาศดังนี้

1. นโยบายและแนวปฏิบัติหลัก

ในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท มีดังต่อไปนี้

1.1 การกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนกลาง (Drive Share) และการใช้งาน Flash Drive / USB รวมถึงเมื่อครบกำหนดเปลี่ยน Password Policy ให้เหมาะสมของบุคลากร

1.2 จัดให้มีระบบสำรองข้อมูลและการบริหารจัดการระบบสารสนเทศที่สามารถรองรับเหตุขัดข้องหรือภัยพิบัติต่างๆ ได้

1.3 ดำเนินการตรวจสอบ ประเมินความเสี่ยงด้านระบบสารสนเทศอย่างสม่ำเสมอและจัดทำแผนป้องกันความเสี่ยงตามที่เหมาะสม

1.4 การนำคอมพิวเตอร์ส่วนตัวมาใช้ภายในบริษัท

1.5 การใช้งานอีเมลบริษัท (Company Email Usage Policy)

1.6 การใช้ Notebook ทรัพย์สินบริษัทในการปฏิบัติงาน และการคืนทรัพย์สินเมื่อพ้นสภาพเป็นพนักงาน

1.7 การใช้งานระบบเครือข่ายของบริษัท (Wi-Fi หรือ LAN) ของอุปกรณ์ส่วนตัว เช่น โทรศัพท์, Tablet

2. การปฏิบัติและการบังคับใช้

จากหัวข้อนโยบายข้างต้น แจ้งแนวทางการปฏิบัติและบังคับใช้ ดังนี้

2.1 การกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนกลาง (Drive Share) และการใช้งาน Flash Drive / USB ต้องมีเอกสารแบบฟอร์มขอเปิดสิทธิ์การใช้งาน ต้องผ่านการอนุมัติระดับจัดการของหน่วยงานต้นสังกัดเท่านั้น

2.2 เมื่อครบกำหนดเวลา 90 วันระบบจะแจ้งให้เปลี่ยน Password เข้าเครื่อง ตาม Policy ความปลอดภัย ต้องเปลี่ยนรหัสผ่านให้ซับซ้อนตามเกณฑ์ ดังนี้ อักษรภาษาอังกฤษตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ผสมตัวเลข และอักขระพิเศษ (!, @, #) อย่างน้อย 8 ตัว

2.2 ระบบสำรองข้อมูลและการบริหารจัดการระบบสารสนเทศ ทางแผนกบริหารสารสนเทศ ได้จัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan) เพื่อรองรับเหตุขัดข้องหรือภัยพิบัติต่างๆ แล้ว

2.3 การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ ทางแผนกบริหารสารสนเทศได้จัดทำแผนป้องกันความเสี่ยงประจำปี 2568-2569 เรียบร้อยแล้ว

2.4 การนำคอมพิวเตอร์ส่วนตัวมาใช้ภายในบริษัท ต้องได้รับอนุญาตจากหัวหน้างานหรือระดับจัดการโดยผ่านเอกสาร Memo และนำเครื่องมาให้แผนกบริหารสารสนเทศทำการตรวจสอบเพื่อความปลอดภัยก่อนนำไปใช้งาน และต้องเป็นไปตามกฎระเบียบ ดังนี้

- ผู้ใช้งานต้องกำหนด Username และ Password สำหรับเข้าใช้งานอุปกรณ์โดยรหัสผ่านต้องมีความซับซ้อนเพียงพอและห้ามเปิดเผยข้อมูลรหัสผ่านแก่บุคคลอื่น
- อุปกรณ์ที่นำมาใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตระบบปฏิบัติการให้เป็นปัจจุบันอยู่เสมอ
- ห้ามติดตั้งและใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ หรือมีความเสี่ยงต่อความปลอดภัยของบริษัท
- การเชื่อมต่อกับเครือข่ายบริษัทต้องเป็นไปตามที่แผนกบริหารสารสนเทศกำหนด เช่น การเชื่อมผ่าน VPN หรือ Wi-Fi ที่กำหนดสำหรับอุปกรณ์บุคคลภายนอก
- ห้ามจัดเก็บและคัดลอกหรือนำข้อมูลสำคัญของบริษัท เช่น ข้อมูลลูกค้า ข้อมูลทางการเงินหรือข้อมูลเชิงกลยุทธ์ ไว้ในอุปกรณ์ส่วนตัว เว้นแต่ได้รับอนุญาติเป็นลายลักษณ์อักษรจากผู้บริหารที่เกี่ยวข้อง
- ฝ่าย IT มีสิทธิ์ตรวจสอบและติดตั้งซอฟต์แวร์ควบคุมความปลอดภัยเพิ่มเติม หากมีความจำเป็นเห็นว่าอุปกรณ์ผู้ใช้งานมีความเสี่ยงและไม่มีความปลอดภัย
- เมื่อสิ้นสุดการปฏิบัติงาน การโอนย้ายตำแหน่ง หรือเมื่อพ้นสภาพจากการเป็นพนักงานบริษัท ผู้ใช้งานต้องลบข้อมูลการใช้ซอฟต์แวร์เพื่อเข้าถึงระบบการทำงานของบริษัทออกจากอุปกรณ์โดยทันที ตามที่แผนกบริหารสารสนเทศกำหนด

ผู้ใดฝ่าฝืนกฎที่กล่าวมาข้างต้นนี้อาจถูกตัดสิทธิ์ในการเข้าถึงระบบงานของบริษัท และอาจถูกดำเนินการทางวินัยตามข้อบังคับของบริษัท รวมถึงอาจมีความผิดทางกฎหมาย หากก่อให้เกิดความเสียหายต่อบริษัท

2.5 การใช้งานอีเมลบริษัท (Company Email Usage Policy) กฎระเบียบ ดังนี้

- อีเมลบริษัทใช้เพื่อการปฏิบัติงาน ห้ามใช้เพื่อวัตถุประสงค์ส่วนตัวที่ไม่เกี่ยวข้องกับการทำงาน
- ห้ามใช้บัญชีอีเมลบริษัทเพื่อสมัครสมาชิกบริการที่ไม่เกี่ยวข้องกับงาน เช่น โซเชียลมีเดีย เกม หรือบริการบันเทิงต่างๆ
- ห้ามส่งเนื้อหาที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ ขัดต่อศีลธรรม หรืออาจก่อให้เกิดความเสียหายต่อชื่อเสียงบริษัท
- ห้ามส่งต่อ เปิดเผย หรือแนบไฟล์ที่เป็นข้อมูลความลับของบริษัทให้บุคคลภายนอกโดยไม่ได้รับอนุญาต
- ห้ามกดลิงก์หรือไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ ผู้ส่งที่ไม่รู้จัก หากมีข้อสงสัย Forward ให้ทีม IT ตรวจสอบก่อนทุกครั้ง
- กรณีผู้ใช้งานทราบรหัสผ่านบัญชีอีเมล ต้องรักษาความปลอดภัยของรหัสผ่านอีเมล และห้ามเปิดเผยให้ผู้อื่นรู้
- แผนกบริหารสารสนเทศ มีสิทธิ์ตรวจสอบการใช้งานอีเมล หากพบว่าบัญชีอีเมลนั้นมีความเสี่ยงต่อบริษัท เพื่อความปลอดภัยของระบบสารสนเทศ
- แผนกบริหารสารสนเทศ มีสิทธิ์ลบหรือปิดบัญชีอีเมลที่ไม่ได้ใช้งาน กรณีพนักงานลาออกแล้ว เว้นแต่หน่วยงานต้นสังกัด แจ้งความจำนงต้องใช้งานบัญชีอีเมลนั้นอยู่

ผู้ใดฝ่าฝืนกฎที่กล่าวมาข้างต้นนี้อาจถูกตัดสิทธิ์การใช้อีเมลของบริษัท และอาจถูกดำเนินการทางวินัยตามข้อบังคับของบริษัท รวมถึงอาจมีความผิดทางกฎหมาย หากก่อให้เกิดความเสียหายต่อบริษัท

2.6 การใช้ Notebook ทรัพย์สินบริษัทในการปฏิบัติงาน และการคืนทรัพย์สินเมื่อพ้นสภาพเป็นพนักงาน

- พนักงานที่รับ Notebook ของบริษัทเพื่อการปฏิบัติงาน ต้องมีเอกสารแบบฟอร์มโอนรับทรัพย์สิน และต้องได้รับอนุมัติจากแผนกทรัพย์สินเท่านั้น
- พนักงานต้องรับผิดชอบต่อการดูแลรักษา Notebook และข้อมูลที่อยู่ในเครื่อง หากเกิดการสูญหายหรือเสียหาย ต้องรายงานต่อฝ่าย IT และหน่วยงานที่เกี่ยวข้องทันที
- ห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต หรือปรับแต่งค่าระบบที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูล
- ห้ามใช้ Notebook ของบริษัทเพื่อการส่วนตัวที่ไม่เกี่ยวข้องกับงาน เช่น เล่นเกม, เข้าเว็บการพนัน, เว็บลามกอนาจาร หรือทำให้เกิดความเสี่ยงด้านความปลอดภัยของบริษัท

2.7 การคืน Notebook เมื่อพ้นสภาพการเป็นพนักงาน

- พนักงานต้องมีเอกสารแบบฟอร์มคืนทรัพย์สิน พร้อมอุปกรณ์ที่รับพร้อมเครื่อง เช่น เมาส์ , สายชาร์จ เป็นต้น และต้องได้รับอนุมัติจากผู้บังคับบัญชา แผนกทรัพย์สิน ตามลำดับ
- แผนก IT มีสิทธิ์ดำเนินการล้างข้อมูล (Data Wipe) เพื่อลบข้อมูลของบริษัทออกทั้งหมดได้
- หากพบความเสียหายหรือสูญหาย พนักงานอาจต้องรับผิดชอบชดใช้ตามระเบียบบริษัท
- บริษัทมีสิทธิ์ระงับการจ่ายค่าชดเชยหรือสิทธิประโยชน์บางส่วนและดำเนินคดีตามกฎหมาย หากว่าพนักงานไม่คืน Notebook ที่เป็นทรัพย์สินของบริษัท จนกว่าจะมีการส่งคืนให้ครบถ้วน

ผู้ใดฝ่าฝืนกฎที่กล่าวมาข้างต้นนี้อาจถูกตัดสิทธิ์การใช้ Notebook ของบริษัท และอาจถูกดำเนินการทางวินัยตามข้อบังคับของบริษัท รวมถึงอาจมีความผิดทางกฎหมาย หากก่อให้เกิดความเสียหายต่อบริษัท

2.8 การใช้งานระบบเครือข่ายของบริษัท (Wi-Fi หรือ LAN) ของอุปกรณ์ส่วนตัว เช่น โทรศัพท์, Tablet

- การนำอุปกรณ์ส่วนตัวเชื่อมต่อเครือข่ายบริษัท ต้องมีแบบฟอร์มการขอใช้บริการ Internet ภายใน ต้องได้รับอนุมัติจากหน่วยงานต้นสังกัดหรือผู้บังคับบัญชาที่เกี่ยวข้องก่อน
- บริษัทมีเครือข่าย **Guest Wi-Fi** แยกต่างหาก สำหรับอุปกรณ์ส่วนตัว เพื่อป้องกันการเข้าถึงเครือข่ายหลัก (Internal Network)
- ห้ามดาวน์โหลด/อัปโหลดไฟล์ที่ผิดกฎหมาย หรือไฟล์ที่มีความเสี่ยง อาจทำให้เครือข่ายบริษัทเสียหาย
- ห้ามเชื่อมต่ออุปกรณ์ส่วนตัวเข้ากับ LAN ภายในบริษัทโดยตรง เว้นแต่ได้รับอนุญาตอย่างเป็นทางการจากหน่วยงานที่เกี่ยวข้อง

ผู้ใดฝ่าฝืนกฎที่กล่าวมาข้างต้นนี้อาจถูกตัดสิทธิ์การใช้งานระบบเครือข่ายของบริษัท และอาจถูกดำเนินการทางวินัยตามข้อบังคับของบริษัท รวมถึงอาจมีความผิดทางกฎหมาย หากก่อให้เกิดความเสียหายต่อบริษัท

นโยบายและการปฏิบัติบังคับใช้ทั้งหมดนี้ เพื่อรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ให้เป็นไปตามระเบียบและวิธีปฏิบัติ ที่บริษัทได้กำหนดไว้ โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้ทำการประเมินไว้

3. การตรวจสอบและประเมินผล

3.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงของสินทรัพย์ ด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง

3.2 หากมีการเปลี่ยนแปลงที่สำคัญด้านระบบงานเทคโนโลยี หรือโครงสร้างองค์กร ต้องทำการประเมินความเสี่ยงใหม่ภายใน 1 เดือน

4. ความรับผิดชอบ

4.1 แผนกเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบหลักในการดำเนินการตามนโยบายนี้

4.2 ต้องทบทวนนโยบายและแนวปฏิบัติให้ทันสมัยอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

4.3 ทุกแผนกและทุกหน่วยงานต้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้เกิดความมั่นคงปลอดภัยในการใช้สารสนเทศของบริษัท

นโยบายนี้ให้ใช้เป็นแนวทางปฏิบัติสำหรับบุคลากรทุกระดับของบริษัท โดยถือเป็นข้อบังคับที่ต้องปฏิบัติตามอย่างเคร่งครัด เพื่อให้บรรลุวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

จึงเรียนมาเพื่อให้นโยบายนี้ ได้ใช้เป็นแนวทางการปฏิบัติต่อไป

ประกาศ ณ วันที่ 24 กันยายน 2568

.....

(.....)

วันที่ ...../...../.....

รองประธานเจ้าหน้าที่บริหาร