ประกาศความเป็นส่วนตัว ด้านความมั่นคงปลอดภัยทางสารสนเทศ

ข้อมูลสารสนเทศของบริษัท เอสพีซีจี จำกัด (มหาชน) และบริษัทในเครือ **("บริษัทฯ")** จัดเป็นสินทรัพย์ทางธุรกิจที่ต้องได้รับการดูแลรักษาอย่างมีประสิทธิภาพ การป้องกันและกำหนด ระดับความปลอดภัยต่อการใช้ข้อมูลภายในจึงมีความสำคัญอย่างยิ่ง กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้ องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ

1. ขอบเขตการบังคับใช้

ประกาศความเป็นส่วนตัว ด้านความมั่นคงปลอดภัยทางสารสนเทศฉบับนี้ มีผลบังคับใช้กับการปฏิบัติงานของพนักงานทุกคน ซึ่งหมายถึง พนักงานประจำ ที่ปรึกษา นักศึกษาฝึกงาน รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคลในนามบริษัทฯ

2. คำนิยาม

2.1 สื่อบันทึกข้อมูล หมายถึง วัสดุที่ใช้สำหรับจัดเก็บข้อมูล เช่น กระดาษ สมุด เทป ซีดี ฮาร์ดดิสก์ เป็นต้น

2.2 สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ หมายถึง วัสดุที่ใช้ในการจัดเก็บข้อมูลซึ่งอยู่ในรูปแบบอิเล็กทรอนิกส์เช่น ฮาร์ดดิสก์ แผ่นดิสก์ ซีดี เทป เอสดีการ์ด เป็นต้น

2.3 อุปกรณ์โมบาย หมายถึง คอมพิวเตอร์พกพา อุปกรณ์ประมวลผลแบบพกพา สมาร์ทโฟน (Smart Phone), แท็บเล็ต (Tablet), เครื่องคอมพิวเตอร์โน๊ตบุ๊ค (Notebook) เป็นต้น

2.4 ทรัพย์สินสารสนเทศ หมายถึง สิ่งที่มีค่าต่อองค์กรซึ่งเกี่ยวข้องกับสารสนเทศ ได้แก่ คอมพิวเตอร์ (Computer), ฮาร์ดแวร์ (Hardware), ซอฟต์แวร์ (Software), ข้อมูลสารสนเทศ ระบบสารสนเทศ สิ่งอำนวยความสะดวกสำหรับการประมวลผล จัดเก็บ และจัดส่ง

3. มาตรการความมั่นคงปลอดภัยสารสนเทศสำหรับพนักงาน (Policy for Employee)

พนักงานมีหน้าที่และความรับผิดชอบที่จะต้องป้องกันและปฏิบัติตามกฎ ระเบียบ ประกาศ และนโยบายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด เพื่อเป็นการป้องกันสารสนเทศ ข้อมูลและทรัพย์สินของบริษัทฯจากความเสี่ยง โดยให้ปฏิบัติ ดังนี้

3.1 การใช้งานทรัพย์สินสารสนเทศ

3.1.1 การเข้าสถานที่ (Physical Access)

บริษัทฯ ได้กำหนดมาตรฐานพื้นที่ออกเป็น 3 ลักษณะ คือ

- พื้นที่ควบคุมความปลอดภัยระดับสูง (High Secure Area)
- พื้นที่ควบคุมสำหรับสำนักงาน (Office Area)

3.1.1 การเข้าสถานที่ (Physical Access) (ต่อ)

- พื้นที่สำหรับผู้มาติดต่อและจัดส่งสิ่งของ (Visitor/Loading Area)

1) ห้ามพนักงานนำพาบุคคลซึ่งไม่มีสิทธิ์เข้าในพื้นที่ควบคุม โดยไม่ได้รับอนุมัติจากผู้มีอำนาจ
2) พนักงานต้องดูแลผู้มาติดต่อซึ่งอยู่ภายใต้ความรับผิดชอบของตน ให้อยู่เฉพาะพื้นที่สำหรับผู้มาติดต่อ เว้นแต่มีความจำเป็นและได้รับการอนุมัติจากผู้ควบคุมพื้นที่ให้สามารถเข้าพื้นที่อื่นได้

3.1.2 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์โมบาย (Computer and Mobile Device Usage)

ห้ามพนักงานนำคอมพิวเตอร์หรืออุปกรณ์โมบายส่วนตัวมาเชื่อมต่อ จัดเก็บ จัดส่ง ประมวลผลข้อมูลของบริษัทฯ เว้นแต่ได้รับอนุมัติจากผู้มีอำนาจ

3.2 การป้องกันทรัพย์สินสารสนเทศ

3.2.1 การจัดชั้นความลับและการจัดการสารสนเทศ

พนักงานต้องจัดชั้นความลับสารสนเทศ (Information Classification) โดยให้เป็นไปตามหลักเกณฑ์และขั้นตอนการปฏิบัติที่กำหนด

3.2.2 การจัดเก็บข้อมูลและสำรองข้อมูล (Information Storing and Backing up)

พนักงานต้องจัดเก็บข้อมูลที่เกี่ยวข้องกับการปฏิบัติงาน ข้อมูลบริษัทฯ หรือข้อมูลอื่นใดตามคำสั่งผู้มีอำนาจ ไว้ในระบบสารสนเทศที่องค์กรกำหนดขึ้น แผนกสารสนเทศจะดำเนินการสำรองข้อมูลในระบบสารสนเทศดังกล่าวทุกวัน เพื่อใช้กรณีมีเหตุจำเป็นต้องกู้คืน

3.2.3 การส่งและการแลกเปลี่ยนข้อมูล (Information Transfer and Exchange)

1) พนักงานที่จำเป็นต้องจัดส่งข้อมูลของบริษัทฯต่อหน่วยงานภายนอกองค์กร ต้องควบคุมการจัดส่งข้อมูลให้เป็นไปตามขั้นตอนการปฏิบัติที่กำหนดขึ้น
2) ห้ามไม่ให้พนักงานส่งข้อมูลของบริษัทฯต่อหน่วยงานภายนอกองค์กรโดยไม่ได้รับอนุมัติจากผู้มีอำนาจ
3) พนักงานต้องใช้เฉพาะอีเมล (E-mail) ช่องทาง (Channel) หรือบริการ (Service) ที่บริษัทฯ กำหนดไว้เพื่อการจัดส่งหรือแลกเปลี่ยนข้อมูล ห้ามไม่ให้ใช้ช่องทางหรือบริการอื่นโดยเด็ดขาด
4) พนักงานต้องป้องกันข้อมูล สารสนเทศที่จัดส่งหรือแลกเปลี่ยนต่อหน่วยงานภายนอกบริษัทฯ โดยให้เป็นไปตามระดับชั้นความลับและขั้นตอนการปฏิบัติที่กำหนด

3.2.4 การใช้งานการเข้ารหัสลับ (Use of Cryptographic)

พนักงานต้องป้องกันข้อมูล สารสนเทศตามระดับชั้นความลับโดยการใช้เทคนิคการเข้ารหัสลับ (Encryption) โดยห้ามไม่ให้พนักงานเปิดเผยกุญแจรหัสลับ (Encryption / Decryption key) ต่อผู้ไม่มีสิทธิ์ หรือ กระทำการโดยประมาทอันเป็นเหตุให้ผู้ไม่มีสิทธิ์ทราบถึงข้อมูลกุญแจรหัสลับ

3.2.5 การเก็บรักษาข้อมูล (Information Retention)

1) พนักงานต้องจัดเก็บข้อมูล บันทึก รวมถึงเอกสารซึ่งอยู่ภายใต้ความรับผิดชอบของตนให้มีความมั่นคงปลอดภัย และเป็นไปตามกฎระเบียบ กฎหมายและขั้นตอนการปฏิบัติที่กำหนด
2) ห้ามไม่ให้พนักงานโยกย้าย ข้อมูล บันทึกหรือเอกสารซึ่งต้องจัดเก็บให้เป็นไปตามกฎ ระเบียบ กฎหมาย โดยเด็ดขาด เว้นแต่ได้รับการอนุมัติให้มีการดำเนินการ

4. มาตรการความมั่นคงปลอดภัยสารสนเทศสำหรับผู้มาติดต่อ (Policy for Visitor) และ ผู้ให้บริการ (Policy for Supplier)

4.1 การใช้งานทรัพย์สินสารสนเทศ

4.1.1 การเข้าสถานที่ (Physical Access)

1) ผู้มาติดต่อต้องแลกบัตรแสดงตนต่อเจ้าหน้าที่รักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบตามที่บริษัทฯกำหนด
2) ผู้มาติดต่อต้องปฏิบัติตามกฎ ระเบียบหรือประกาศ ทั้งด้านความปลอดภัย อาชีวอนามัย ความมั่นคงปลอดภัยสารสนเทศหรืออื่นใดที่บริษัทฯ กำหนดอย่างเคร่งครัด
3) ห้ามไม่ให้ผู้มาต่อติดทำการบันทึกภาพ เสียง ภาพนิ่ง ภายในพื้นที่ของบริษัทฯ โดยไม่ได้รับอนุญาต
4) ผู้มาติดต่อต้องอยู่ที่พื้นที่ สถานที่ ซึ่งหน่วยงานหรือพนักงานผู้รับผิดชอบจัดให้เท่านั้น
5) ห้ามไม่ให้ผู้มาติดต่อเข้าพื้นที่อื่นใด ที่ไม่ได้รับอนุญาตโดยเด็ดขาด

4.2 การป้องกันทรัพย์สินสารสนเทศ

4.2.1 การใช้เครือข่าย (Network Usage)

ห้ามผู้มาติดต่อทำการต่อเชื่อม คอมพิวเตอร์หรืออุปกรณ์อื่นใดกับเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาต

4.2.2 การส่งและการแลกเปลี่ยนข้อมูล (Information Transfer and Exchange)

1) ผู้ให้บริการต้องติดต่อที่จำเป็นต้องรับหรือส่งข้อมูลกับพนักงานของ บริษัทฯ ให้รับหรือส่งข้อมูลผ่านที่อยู่อีเมล (Email) หรือช่องทาง (Channel) ที่เป็นทางการของบริษัทฯเท่านั้น เว้นแต่เป็นการติดต่อในเรื่องส่วนตัว
2) ผู้ให้บริการต้องควบคุมการเปิดเผยข้อมูลหรือสารสนเทศของบริษัทฯแก่พนักงานหรือหน่วยงานที่ตนจ้างเพื่อให้บริการ ผู้ให้บริการจะปฏิเสธความรับผิดชอบต่อการรักษาความลับหรือการเผยแพร่ข้อมูลไม่ได้ และหากเกิดความเสียหายจะต้องชดใช้ตามที่กำหนดไว้ในสัญญา

5. โทษของการไม่ปฏิบัติตามประกาศความเป็นส่วนตัว ด้านความมั่นคงปลอดภัยทางสารสนเทศ

ผู้เกี่ยวข้องทั้งภายในและภายนอก ต้องทำความเข้าใจแนวทางปฏิบัติตามอย่างเคร่งครัด หากฝ่าฝืนหรือไม่ปฏิบัติตาม จำเป็นต้องได้รับบทลงโทษตามที่กำหนด

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 30 พฤษภาคม 2565

(ดรวันดี กุญชรยาคง จุลเจริญ)
กรรมการผู้จัดการใหญ่