

แนวนโยบายและแนวปฏิบัติ ในการรักษาความปลอดภัยระบบสารสนเทศ V4.0

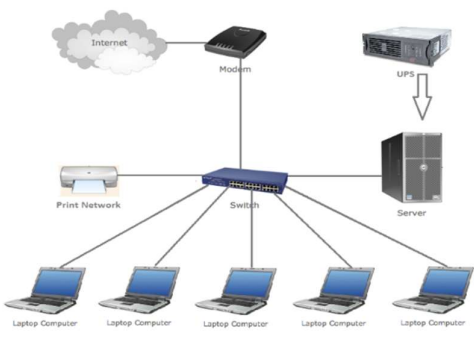
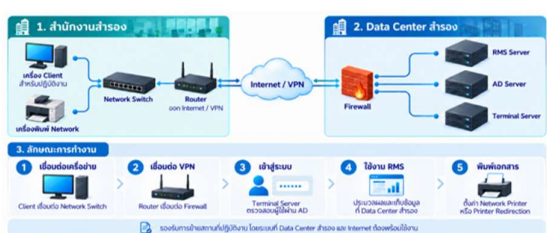
บริษัท แอล.พี.เอ็น. ดีเวลลอปเม้นท์ จำกัด (มหาชน)

และบริษัทในเครือ

มีผล 1 ตุลาคม 2569

ประวัติการปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศ

เวอร์ชัน	รายการปรับปรุงแก้ไข/เพิ่มเติม	ประเภท	วันที่
4	หมวด 7 นโยบายการสำรองข้อมูล 1. ข้อ 7.5 เพิ่มข้อความ หน่วยงานสารสนเทศต้องจัดให้มีการจัดเก็บข้อมูลสำรองอย่างน้อย 2 แห่งฯลฯ	เพิ่มเติม	1 ต.ค. 2569
	แผนรองรับสถานการณ์ฉุกเฉิน 1. ข้อ 3.1.1 เปลี่ยนแปลง ดังนี้ <u>เดิม</u> ระบุเป็น ศูนย์อบรม P.S.T City Home <u>ใหม่</u> ระบุเป็นที่ติดตั้ง Server ใช้บริการ Co-Location หรือ Private Cloud 2. ข้อ 3.1.2 เปลี่ยนแปลง ดังนี้ <u>เดิม</u> ระบุเป็น สำนักงานกลางสาขา <u>ใหม่</u> ระบุเป็น สถานที่ตั้ง Client สำหรับการปฏิบัติงาน เลือกตามความเหมาะสมดังนี้ • ศูนย์อบรม P.S.T. City Home • สำนักงานขายโครงการ 3. ข้อ 3.1.3 ตัดออก <u>เดิม</u> ระบุเป็น สำนักงานขายโครงการ (ตามความเหมาะสม) <u>ใหม่</u> ระบุอยู่ในข้อ 3.1.2 4. ข้อ 3.1.4 ตัดออก <u>เดิม</u> ระบุเป็น ผู้ให้บริการ Co-location หรือ Private Cloud (ตามความเหมาะสม) <u>ใหม่</u> ระบุอยู่ในข้อ 3.1.1 5. ข้อ 4.1 แก้ไข ผู้รับผิดชอบขนย้ายอุปกรณ์ Server, Network และ Firewall <u>เดิม</u> ระบุเป็นรายชื่อตามที่กำหนด <u>ใหม่</u> ระบุเป็นผู้ทำหน้าที่ System	ปรับปรุง	

เวอร์ชัน	รายการปรับปรุงแก้ไข/เพิ่มเติม	ประเภท	วันที่						
4	Administrator และ ผู้ดูแลระบบที่เกี่ยวข้อง 6. ข้อ 4.2 แก้ไข ผู้รับผิดชอบประสานงานจัดหา Hardware/Software <u>เดิม</u> ระบุเป็นรายชื่อตามที่กำหนด <u>ใหม่</u> ระบุเป็นผู้ทำหน้าที่ IT Support, และ HW Support 7. ข้อ 5. แก้ไข Diagram รองรับการกู้คืนระบบหลักให้สอดคล้องกับรูปแบบการกู้คืน พร้อมคำอธิบาย <u>เดิม</u>  <u>ใหม่</u>  <table><tr><th>1.สำนักงานสำรอง</th><th>2.Data Center สำรอง</th><th>3.ลักษณะการทำงาน</th></tr><tr><td>สถานที่ที่เก็บข้อมูลต่างๆ เข้าปฏิบัติงานชั่วคราว โดยมีการเตรียมความพร้อมระบบงาน และอุปกรณ์เท่าที่จำเป็น</td><td>Co-Location/Private Cloud ที่ใช้เป็น Data Center สำรอง เพื่อเก็บข้อมูลระบบ RMS และเชื่อมต่อกับสำนักงานสำรอง</td><td>ผู้ใช้งานจากสำนักงานสำรองเชื่อมต่อเครือข่ายผ่าน VPN ไปยัง Data Center สำรอง และเปิดใช้ระบบ RMS ตามปกติ</td></tr></table>	1.สำนักงานสำรอง	2.Data Center สำรอง	3.ลักษณะการทำงาน	สถานที่ที่เก็บข้อมูลต่างๆ เข้าปฏิบัติงานชั่วคราว โดยมีการเตรียมความพร้อมระบบงาน และอุปกรณ์เท่าที่จำเป็น	Co-Location/Private Cloud ที่ใช้เป็น Data Center สำรอง เพื่อเก็บข้อมูลระบบ RMS และเชื่อมต่อกับสำนักงานสำรอง	ผู้ใช้งานจากสำนักงานสำรองเชื่อมต่อเครือข่ายผ่าน VPN ไปยัง Data Center สำรอง และเปิดใช้ระบบ RMS ตามปกติ	ปรับปรุง	1 ต.ค. 2569
1.สำนักงานสำรอง	2.Data Center สำรอง	3.ลักษณะการทำงาน							
สถานที่ที่เก็บข้อมูลต่างๆ เข้าปฏิบัติงานชั่วคราว โดยมีการเตรียมความพร้อมระบบงาน และอุปกรณ์เท่าที่จำเป็น	Co-Location/Private Cloud ที่ใช้เป็น Data Center สำรอง เพื่อเก็บข้อมูลระบบ RMS และเชื่อมต่อกับสำนักงานสำรอง	ผู้ใช้งานจากสำนักงานสำรองเชื่อมต่อเครือข่ายผ่าน VPN ไปยัง Data Center สำรอง และเปิดใช้ระบบ RMS ตามปกติ							

เวอร์ชัน	รายการปรับปรุงแก้ไข/เพิ่มเติม	ประเภท	วันที่
4	8. ข้อ 6. แก้ไข ขั้นตอนดำเนินการกู้คืนระบบ กรณีเกิดเหตุฉุกเฉิน ดังนี้ <u>เดิม</u> แบ่งเป็น 5 ขั้นตอน <u>ใหม่</u> แบ่งเป็น 3 ขั้นตอน ขั้นตอน 1 แก้ไขขั้นตอนเป็นการติดตั้งอุปกรณ์ คอมพิวเตอร์ และเน็ตเวิร์คของสำนักงานสำรอง ระยะเวลาดำเนินการ 3-6 ชม. ขั้นตอน 2 แก้ไขขั้นตอนเป็นการติดตั้ง Server ที่ Data Center สำรอง สำหรับกู้คืนข้อมูล ระบบRMS และเชื่อมต่อกับสำนักงานสำรอง ระยะเวลาดำเนินการ 3-6 ชม. ขั้นตอน 3 แก้ไขขั้นตอนเป็นการทดสอบการใช้งาน ณ สำนักงานสำรอง ระยะเวลา ดำเนินการ 1-2 ชม.	ปรับปรุง	1 ต.ค. 2569
	คู่มือการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน 1. อัปเดตรายชื่อ หมายเลขติดต่อผู้เกี่ยวข้อง	ปรับปรุง	
3	หมวด 4 การบริหารจัดการทรัพย์สินขององค์กร ใช้ E-Mail บริษัทลงทะเบียนโปรแกรมละเมิดลิขสิทธิ์ ถือเป็นความรับผิดชอบของพนักงาน	เพิ่มเติม	2 ก.พ. 2568
	หมวด 11 การปฏิบัติตามข้อกำหนด การปฏิบัติงานให้ครอบคลุม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วย (11.1)	เพิ่มเติม	
	ภาคผนวก 1. ปรับปรุงผู้รับผิดชอบ, หมายเลขติดต่อเมื่อเกิดสถานการณ์ฉุกเฉิน (4) , (2) ปรับปรุงมาตรฐานการจัดเก็บข้อมูลของส่วนกลาง ระดับองค์กร ระดับทีม ระดับฝ่าย และส่วนตัว ใน MS 365 แทน Drive M,N,O (5)	ปรับปรุง	

เวอร์ชัน	รายการปรับปรุงแก้ไข/เพิ่มเติม	ประเภท	วันที่
2	ปรับปรุง หมวด 8 การควบคุมการเข้าถึง เพิ่มเนื้อหาให้ครอบคลุมถึงการใช้อุปกรณ์ส่วนตัว และปรับปรุงการจัดการการเข้าถึงระบบของผู้ใช้งาน ตาม Comment ของ External Audit ปรับปรุงระบบรักษาความปลอดภัยให้รองรับ PDPA (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ 1 มิ.ย. 65) 1.มาตรการด้าน Hardware (8) 2. มาตรการด้าน Software (8) 3. การประมวลผลระบบสารสนเทศ (9.2) 4. การวางระบบทางด้าน Software (11.1) 5. การวางระบบด้าน Peopleware (11.1)	เพิ่มเติม	1 ก.ค. 2565
	แก้ไขภาคผนวก 1. ปรับปรุงแผนรองรับสถานการณ์ฉุกเฉิน 1. ปรับปรุงผู้รับผิดชอบเมื่อเกิดเหตุฉุกเฉิน (4) 2. ปรับปรุงขั้นตอนการกู้คืนระบบกรณีเกิดเหตุให้สอดคล้องกับวิธีการ Backup แบบใหม่ (6) 3. ปรับปรุงการดำเนินการเมื่อเกิดเหตุฉุกเฉิน (1) 2. Update Firewall Policy	ปรับปรุง	
1	ร่างนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศ	จัดทำ	1 ม.ค. 2559

คำนำ

การจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้เพื่อให้การดำเนินการใดๆด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้

ทั้งนี้ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศถือเป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่องและจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่ายนอกจากนั้นยังต้องมีการตรวจสอบอย่างสม่ำเสมอเพื่อปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อให้ระบบสารสนเทศของบริษัทเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องซึ่งอาจส่งผลให้ถูกคุกคามจากภัยต่างๆ

ดังนั้นบริษัทจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อเผยแพร่ให้ผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกได้รับทราบ และขอความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดต่อไป

วัตถุประสงค์

1. เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของบริษัทและ
เป็นไปตามกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง อาทิ เช่น
 - พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
 - พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
 - พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
 - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 - ประกาศกฎกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทาง
คอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2562
2. เพื่อกำหนดแนวทางและวิธีการปฏิบัติสำหรับพนักงาน หรือบุคคลที่ปฏิบัติงานให้กับบริษัท
3. เพื่อให้พนักงานทุกคนได้ตระหนัก เข้าใจในบทบาทหน้าที่ของตน ร่วมกันดูแลรักษา และใช้ระบบ
สารสนเทศให้เกิดประโยชน์สูงสุดต่อองค์กร และมีความมั่นคงปลอดภัย
4. เพื่อลดความเสี่ยง และเตรียมความพร้อมเมื่อเกิดเหตุการณ์ฉุกเฉิน รักษาความต่อเนื่องของธุรกิจ
5. เพื่อให้เกิดความมั่นใจในระบบสารสนเทศทั้งภายในและภายนอกองค์กร
6. เพื่อปกป้องข้อมูลที่มีความสำคัญต่อธุรกิจ ระบบเทคโนโลยีสารสนเทศ และทรัพยากรดิจิทัลอื่นๆ

สารบัญ

	หน้า
หมวด 1 ความหมาย และคำจำกัดความ	9
หมวด 2 นโยบายความมั่นคงปลอดภัย	12
หมวด 3 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร	13
หมวด 4 การบริหารจัดการทรัพย์สินขององค์กร	14
หมวด 5 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร	20
หมวด 6 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม	22
หมวด 7 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายขององค์กร	24
หมวด 8 การควบคุมการเข้าถึง	29
หมวด 9 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ	34
หมวด 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร	36
หมวด 11 การปฏิบัติตามข้อกำหนด	36
เอกสารแนบ 1 แผนรองรับสถานการณ์ฉุกเฉิน	39
เอกสารแนบ 2 แนวปฏิบัติเมื่อเกิดเหตุฉุกเฉิน	42
เอกสารแนบ 3 แนวปฏิบัติในการใช้งานระบบคอมพิวเตอร์ และอินเทอร์เน็ต	44

หมวด 1

ความหมายและคำจำกัดความ

“**สินทรัพย์คอมพิวเตอร์**” หมายถึง สินทรัพย์ทุกอย่างที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล เป็นต้น

“**ระบบเครือข่าย**”(Network System) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของบริษัท

“**คอมพิวเตอร์แม่ข่าย**” (Server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์สำหรับให้บริการแก่เครื่องคอมพิวเตอร์ หรือควบคุมการทำงานในเครือข่าย

“**การเข้าถึงเครือข่ายจากระยะไกล**” หมายถึง การที่เครื่องคอมพิวเตอร์หรือระบบเครือข่าย เชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสารหรือสื่อสัญญาณอื่น ๆ อาทิ Modem, VPN

“**การควบคุมการเข้าถึง**” (Access Control) หมายถึง การควบคุมการเข้าถึงหรือใช้งานสินทรัพย์คอมพิวเตอร์ ให้เป็นไปตามสิทธิที่กำหนดไว้เท่านั้น

“**เครื่องคอมพิวเตอร์**” หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลทำงานด้วยระบบอิเล็กทรอนิกส์โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ อาทิ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพาได้ (Notebook Computer)

“**อุปกรณ์คอมพิวเตอร์**” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์ เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ และให้รวมถึงเครื่องคอมพิวเตอร์

“**สื่อสัญญาณ**” หมายถึง สื่อกลางใด ๆ ที่ใช้เชื่อมต่อระหว่างอุปกรณ์คอมพิวเตอร์ อาทิ สายทองแดง สายใยแก้วนำแสง เครือข่ายไร้สาย (Wifi)

“**ฮาร์ดแวร์**” หมายถึง อุปกรณ์คอมพิวเตอร์

“**ซอฟต์แวร์**” หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงานตามต้องการ

“**ซอฟต์แวร์ระบบ**” หมายถึง ซอฟต์แวร์ที่ควบคุมการทำงานของอุปกรณ์คอมพิวเตอร์ เช่น ระบบปฏิบัติการ

“**ซอฟต์แวร์ประยุกต์**” หมายถึง ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้กับงานเฉพาะด้านตามความต้องการ อาทิ ซอฟต์แวร์สำหรับพิมพ์เอกสาร ซอฟต์แวร์สำหรับการคำนวณทางบัญชี

“**ระบบเทคโนโลยีสารสนเทศ**” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร

การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ อาทิ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ระบบงาน และสารสนเทศ

“สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้

“ระบบงาน” หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงาน เพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบจัดเก็บเอกสาร ระบบบัญชี

“ระบบปฏิบัติการ” (Operating System) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของ เครื่องคอมพิวเตอร์ และ จัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุม การทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

“ระบบป้องกันการบุกรุก” (Firewall) หมายถึง ระบบรักษาความปลอดภัยที่ประกอบด้วยกลุ่มอุปกรณ์คอมพิวเตอร์ และซอฟต์แวร์ซึ่งทำหน้าที่ป้องกันผู้ไม่ได้รับอนุญาตจากเครือข่ายภายนอกเข้าใช้ระบบ และจำกัดการใช้งานของผู้ใช้งานภายในให้เป็นไปตามนโยบายที่บริษัทกำหนด

“ข้อมูล” หมายถึง ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ สร้าง สั่ง รับ เก็บรักษา หรือประมวลผล ได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์คอมพิวเตอร์ และให้

รวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ไฟล์” (File) หมายถึง ข้อมูลที่ถูกรวบรวมลงสื่อบันทึกและระบุเป็นหนึ่งหน่วยโดยมีชื่อเฉพาะ เช่น ซอฟต์แวร์ใช้งาน และไฟล์เอกสารต่าง ๆ ที่สร้างขึ้นและใส่ชื่อให้แก่ไฟล์นั้นแล้วเก็บบันทึกลงสื่อบันทึก เป็นต้น

“ผู้ใช้งาน” (User) หมายถึง เจ้าหน้าที่หรือบุคคลภายนอกที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท

“ผู้บริหารเครือข่าย” (Network Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและบำรุงรักษา เครือข่าย

“ผู้บริหารคอมพิวเตอร์แม่ข่าย” (Host/Server Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแล และบำรุงรักษาคอมพิวเตอร์แม่ข่าย

“ผู้บริหารระบบป้องกันการบุกรุก” (Firewall Administrator) หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบในการดูแลและ บำรุงรักษาระบบป้องกันการบุกรุก

“บัญชีผู้ใช้งาน” (User Name) หมายถึง บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่ง
เป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบเทคโนโลยีสารสนเทศ

“บัญชีผู้บริหารคอมพิวเตอร์แม่ข่าย” (Administrator Account) หมายถึง บัญชีที่ผู้บริหารคอมพิวเตอร์แม่ข่ายใช้
ในการบริหารระบบคอมพิวเตอร์แม่ข่าย

“บัญชีผู้ใช้งานอีเมล” (Email Account) หมายถึง บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงระบบเมลของบริษัท

“เอกสารโครงแบบ” (Configuration Document) หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่างๆ ใน
ระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศใช้งานได้ตามความต้องการ

“ความเสี่ยง” หมายถึง โอกาสของสินทรัพย์คอมพิวเตอร์ในการถูกละเมิดการรักษาความปลอดภัย

“เหตุการณ์ผิดปกติ” (Incident) หมายถึง เหตุการณ์ใด ๆ ที่มีผลกระทบต่อการรักษาความปลอดภัยของระบบ
เทคโนโลยีสารสนเทศ

“เจ้าหน้าที่” หมายถึง พนักงานในบริษัท

“ส่วนงาน” หมายถึง ฝ่ายตามโครงสร้างของบริษัท

“โปรแกรมประสงค์ร้าย” หมายถึง ฮาร์ดแวร์ หรือซอฟต์แวร์ที่มีการตั้งใจใส่เข้าไปในระบบโดยไม่ได้รับอนุญาต
เพื่อให้ทำงานตามความประสงค์ของผู้ประสงค์ร้าย ซึ่งมีผลให้คอมพิวเตอร์ หรือ ระบบเทคโนโลยีสารสนเทศ หรือ
ชุดคำสั่งอื่นได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตาม
คำสั่งที่กำหนดไว้

“หน่วยงานภายนอก” หมายถึง องค์กรซึ่งบริษัท อนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้งานระบบ
เทคโนโลยีสารสนเทศของบริษัท โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผย
ความลับของบริษัทโดยไม่ได้รับอนุญาต

หมวด 2

นโยบายความมั่นคงปลอดภัย

เมื่อประกาศฉบับนี้มีผลบังคับใช้ ให้หน่วยงานสารสนเทศ เป็นผู้ทำหน้าที่ในการออกระเบียบปฏิบัติ ข้อกำหนด ข้อบังคับต่างๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและ เครือข่ายคอมพิวเตอร์ของบริษัทโดยความเห็นชอบจากผู้บริหารระดับสูง และผู้บริหารระดับสูงให้การสนับสนุนในเรื่องนโยบาย งบประมาณ ทรัพยากรและอื่นๆ ที่จำเป็นเพื่อให้การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์มีการพัฒนาและปรับปรุงอย่างต่อเนื่อง

ต้องจัดให้มีการเผยแพร่นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ให้กับเจ้าหน้าที่ และผู้ที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ

ต้องดำเนินการทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยี สารสนเทศและ เครือข่ายคอมพิวเตอร์อย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อการรักษาความมั่นคง ปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัท

หมวด 3

โครงสร้างทางด้านการมั่นคงปลอดภัยสำหรับองค์กร

3.1 โครงสร้างทางด้านการมั่นคงปลอดภัยสารสนเทศภายในองค์กร

ผู้บริหารระดับสูงเป็นผู้กำหนดให้มีตัวแทนหรือคณะทำงานจากหน่วยงานต่างๆ ภายในบริษัท เพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัทโดยที่ตัวแทนหรือคณะทำงานเหล่านั้น จะต้องมีการกำหนด หน้าที่ความรับผิดชอบในการดำเนินงานทางด้านการมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กรอย่างชัดเจน

ตัวแทนหรือคณะทำงานซึ่งถูกแต่งตั้งโดยผู้บริหารระดับสูง เป็นผู้รับผิดชอบในการบริหารจัดการและควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่าย คอมพิวเตอร์ขององค์กร ตลอดจนทบทวนนโยบายระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำขั้นตอนและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ต่างๆ และเอกสารที่เกี่ยวข้องในการจัดทำ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่ของบริษัทต้องไม่เปิดเผยความลับของบริษัท เว้นแต่จะได้รับการอนุญาตให้เปิดเผยจากบริษัท

ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการการดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์โดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท

3.2 โครงสร้างทางด้านการมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือ หน่วยงานภายนอก

ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ใน การประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

ต้องระบุและบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท เมื่อมีความจำเป็นต้องให้บุคคลภายนอก หรือหน่วยงานภายนอก หรือผู้ให้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศของบริษัทก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวด 4

การบริหารจัดการทรัพย์สินขององค์กร

4.1 ความรับผิดชอบต่อสินทรัพย์

ต้องมีการจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อบริษัทให้ถูกต้องอยู่เสมอ รวมทั้งมีการระบุความเป็นเจ้าของในทรัพย์สินต่างๆ ต้องจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศ และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น อาทิ อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่

ต้องมีการเก็บรักษาทรัพย์สินที่มีความสำคัญต่อบริษัทอย่างเป็นระเบียบในสถานที่ที่ปลอดภัยให้เหมาะสม

การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่บริษัท เป็นผู้จัดทำมานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการปฏิบัติงานตามภารกิจของบริษัทการใช้งานระบบและอุปกรณ์ต่างๆ เพื่อกิจธุระส่วนตัวนั้นอนุญาตให้สามารถใช้ได้ในขอบเขตตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
- เจ้าหน้าที่ ตลอดจนบุคคลและ/หรือนิติบุคคลที่ได้รับว่าจ้างโดยบริษัท จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านั้นให้มีความปลอดภัย และคงความถูกต้อง โดยหมายความรวมถึงข้อมูล และระบบสารสนเทศของบริษัท
- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของบริษัท อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน
- เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด

ของบริษัทต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้ง เมื่อต้องการใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง

- กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบอุปกรณ์คอมพิวเตอร์ของบริษัทที่ได้รับมอบหมาย
- ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้ากับระบบเครือข่ายของบริษัทรวมถึง ต้องไม่ติดตั้งซอฟต์แวร์ใดๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทก่อนได้รับอนุญาตจากผู้จัดการฝ่าย ต้นสังกัดและจากหน่วยงานสารสนเทศเป็นลายลักษณ์อักษร
- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้อง เทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัท อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ
- อุปกรณ์คอมพิวเตอร์ของบริษัท ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้นๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด

การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัท
- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัท ทั้งที่ได้มาจากการพัฒนาขึ้นโดยผู้ใช้งาน หรือที่ได้รับการจัดซื้อจะต้องได้รับการตรวจสอบควบคุม และอนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของบริษัท
- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของบริษัทมีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งาน ต้องได้รับ

การจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้ว่าการสารสนเทศเพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านั้นมีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของบริษัทเท่านั้น

การอนุญาตให้ใช้งานอินเทอร์เน็ตดังนี้

- บริษัทจัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการค้นหาข้อมูลความรู้และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของบริษัท
- ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้บริษัทและบุคคลผู้ที่เกี่ยวข้องกับบริษัทเสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านช่องทาง (Gateway) ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัทขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อปอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมัลแวร์แฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสม หรือผิดกฎหมาย
- บริษัทไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (อาทิ ผ่านทางเว็บบอร์ด, บล็อก หรือโซเชียล มีเดียต่างๆ) ของเจ้าหน้าที่ ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

การอนุญาตให้ใช้งานอีเมลดังนี้

- ผู้ใช้งานอีเมลของบริษัท ต้องมี E-Mail Account เป็นของตนเอง
- E-Mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล้วงละเมิด และการนำอีเมลไปใช้ในทางที่ผิด

- E-Mail Account ที่มีวัตถุประสงค์พิเศษ อาจได้รับการสร้างขึ้นเพื่อเป็น E-Mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยผู้เข้าใช้งาน จะต้องได้รับการอนุญาตจากผู้จัดการฝ่ายโดยตรงและผู้จัดการฝ่ายสารสนเทศ ก่อนให้สิทธิ์เข้าใช้งาน ทุกครั้ง
- E-Mail Account ทั้งหมด และอีเมลทุกฉบับ (รวมถึงอีเมลส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่ บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท ถือเป็นสินทรัพย์ของบริษัท
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือติดต่อสื่อสารกับ ระบบอีเมลของบริษัท
- พื้นที่เก็บอีเมลบนระบบ MS 365 (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณ ของอีเมลมากจนใกล้เคียงกับขนาดพื้นที่ที่กำหนดไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมลมากเกินไป พื้นที่จัดเก็บแล้วผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมล ได้ ตามปกติอีกต่อไป
- ผู้ใช้งานต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บ อีเมลให้เป็นไปตามขนาดที่บริษัทกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงาน และอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-Mail Account ของบริษัทเพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่าง อาทิ เพื่อการโฆษณาชวนเชื่อ สิ่งผิดกฎหมาย สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ การ เผยแพร่ภาพลามกอนาจาร เป็นต้น
- ห้ามใช้ E-Mail Account ของบริษัทเพื่อกระทำการใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ซอฟต์แวร์ หรือมีความเสี่ยง อาทิเช่น ลงทะเบียนติดตั้งซอฟต์แวร์บนเครื่องส่วนตัว ลงทะเบียนใช้งาน ซอฟต์แวร์ออนไลน์ที่บริษัทไม่มีลิขสิทธิ์ การลงทะเบียนต่างๆ บนเว็บไซต์ใดๆ ที่ไม่ใช่ของบริษัท ถือเป็น ความรับผิดชอบของพนักงาน
- ห้ามใช้ E-Mail Account ของบริษัทในการประกาศข้อมูลใดๆ ในชุมชนอิเล็กทรอนิกส์ อาทิ เว็บไซต์ บอร์ด บล็อก กระดานข่าว เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงาน ให้กับบริษัท
- การใช้งานอีเมลต้องได้รับการตั้งค่าให้อีเมลส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็น

นั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน ชื่อบริษัทและเบอร์โทรศัพท์ติดต่อ

- ห้ามผู้ใช้งานทำสำเนาข้อความหรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมลของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมลนั้นในนามตัวแทนของบริษัท
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมลหรือ E-Mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-Mail Account ของตนโดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ ตัวอย่าง อีเมลขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail)
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งอีเมลหลอกลวง หรือการส่งอีเมลในลักษณะถูกโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาทกล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ช่มชู้ ลามกอนาจาร การยั่วยู่ทางเพศ หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติหรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัท
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์ หรือโปรแกรมแฝง Malware (ม้าโทรจัน)
- เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมลโดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

การอนุญาตให้ใช้งานโทรศัพท์ โทรสาร เครื่องพิมพ์ และเครื่องถ่ายเอกสาร มีดังนี้

- ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิดพลาดเลขผิดส่วนงาน เป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น

- ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรองรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

4.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ

ต้องจัดให้มีวิธีการจัดทำและการจ่ายซื้อสำหรับปิดฉลากเอกสารข้อมูล และอุปกรณ์ สินทรัพย์สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศ

ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อกได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ อาทิ เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร โดยทันที

เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่มีการเปิดเผยนั้น ครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

เจ้าหน้าที่ต้องไม่พูดคุย หรือใช้งานข้อมูลลับของบริษัทในพื้นที่สาธารณะ อาทิ ลิฟท์ ร้านอาหาร สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (อาทิ Tablet, Thumb-Drive, CD-Rom) ที่มีข้อมูลลับของบริษัทบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง ข้อมูลสำคัญที่เกี่ยวข้องกับการดำเนินงานของบริษัททั้งหมด ทั้งที่มีการเก็บรักษาอยู่ในเครื่อง คอมพิวเตอร์ของผู้ใช้งานหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ดูแลโดยผู้ใช้งานต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาใดๆ เกิดขึ้น ตัวอย่าง การติดไวรัส ฮาร์ดดิสก์เสีย

หมวด 5

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

5.1 การสร้างความความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากรก่อนการทำงาน

หน่วยงานภายนอกที่ได้รับการว่าจ้างตามสัญญาการจ้างงานต้องปฏิบัติตามมาตรการ รักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยของบริษัทอย่างเคร่งครัด

5.2 การสร้างความมั่นคงปลอดภัยขณะเป็นพนักงาน

เจ้าหน้าที่ หรือผู้ใช้งานมีหน้าที่ศึกษาทำความเข้าใจวิธีปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่บริษัทกำหนด เพื่อนำไปปฏิบัติในการรักษาความปลอดภัยสินทรัพย์คอมพิวเตอร์ในส่วนที่ตนใช้งานหรือดูแลรับผิดชอบ

ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่และลูกจ้างเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้าง ความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศของบริษัทด้วย เจ้าหน้าที่และลูกจ้างใหม่ทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคง ปลอดภัยระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อน หรืออย่างน้อยภายใน 30 วัน นับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ

ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของบริษัท แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุ ในแต่ละข้อกฎหมายนั้น ๆ

5.3 การยกเลิกการจ้างงาน

เพื่อให้การบริหารจัดการ Login หรือ User ID เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด หน่วยงานด้านทรัพยากรบุคคลต้องแจ้งให้หน่วยงานสารสนเทศทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่ และลูกจ้าง

- การโยกย้ายหน่วยงาน
- การพักผ่อน การลางโหวทางวินัย หรือระงับการปฏิบัติหน้าที่

เจ้าหน้าที่และลูกจ้างซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับ ระบบงาน คอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

หลังจากมีการยกเลิกหรือเปลี่ยนแปลงตำแหน่งการเป็นเจ้าหน้าที่และลูกจ้างแล้ว จะต้องแจ้งยกเลิก การเข้าถึงข้อมูลต่าง ๆ ของหน่วยงาน และจะแจ้งต่อเจ้าหน้าที่ และลูกจ้างอื่น ๆ, ลูกค้า, บริษัทคู่ค้า, ที่ เกี่ยวข้องให้รับทราบตามความเหมาะสม

หมวด 6

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

6.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

ให้หน่วยงานสารสนเทศเป็นผู้กำหนดรายละเอียดของสถานที่ อุปกรณ์ ป้องกัน ความเสียหาย และการควบคุมการเข้าออกในเขตรักษาความปลอดภัยให้เหมาะสมกับสถานที่ หรือพื้นที่ ที่ต้องรักษาความปลอดภัยที่เหมาะสม

ต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ ที่ต้องการรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น หากมีบุคคลอื่นใดที่ไม่ใช่ “เจ้าหน้าที่หน่วยงานสารสนเทศ” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานสารสนเทศจะต้องจัดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกห้อง คอมพิวเตอร์ ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน

ต้องไม่ยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สำนักงานโดยเด็ดขาดเว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงานและพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ อาทิ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สำนักงานหรือห้องจะต้อง ไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตูหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่

ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด

ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม

เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บรักษาสินทรัพย์คอมพิวเตอร์ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือภัยอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ พร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในเขตรักษาความปลอดภัยอย่างน้อยปีละ 1 ครั้ง จัดอบรมและซักซ้อมเจ้าหน้าที่ปฏิบัติงานภายในเขตรักษาความปลอดภัยตามระยะเวลาอันสมควร เพื่อให้สามารถใช้งานอุปกรณ์รักษาความปลอดภัยได้อย่างถูกต้องและเหมาะสม

ให้หน่วยงานสารสนเทศรับผิดชอบในการบำรุงรักษาสถานที่อุปกรณ์ป้องกันความเสียหาย และอุปกรณ์ป้องกันภัยต่างๆ ภายในเขตรักษาความปลอดภัยตามระยะเวลาอันสมควร

ให้หน่วยงานสารสนเทศจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาใน พื้นที่ได้

6.2 ความมั่นคงปลอดภัยของอุปกรณ์

เจ้าหน้าที่หรือผู้ใช้งานต้องจัดวางและป้องกันอุปกรณ์ของบริษัทเพื่อลดความเสี่ยงจากภัย คุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

กำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่าง ต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

เจ้าหน้าที่หรือผู้ใช้งานต้องทำการประสานงานกับหน่วยงานสารสนเทศในการจัดเตรียมแผนรองรับหากอุปกรณ์คอมพิวเตอร์ได้รับความเสียหายและทดสอบแผนรองรับตามระยะเวลาอันสมควร

เจ้าหน้าที่หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและ ซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทึบก่อนที่จะทิ้งอุปกรณ์ หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุง ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าว

มอบหมายให้เจ้าหน้าที่ในส่วนงานดูแลการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และควบคุมการ ขนย้ายอุปกรณ์คอมพิวเตอร์ เพื่อป้องกันข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์รั่วไหลหรือถูกแก้ไข

หมวด 7

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

7.1 การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงาน

ให้หน่วยงานสารสนเทศจัดทำคู่มือ และ/หรือขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วย รายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ

ให้หน่วยงานสารสนเทศมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ทุกครั้ง

ให้หน่วยงานสารสนเทศและการสื่อสารบันทึกการเปลี่ยนแปลงทุกครั้ง โดยจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบรายละเอียดของการเปลี่ยนแปลง ให้หน่วยงานสารสนเทศ กำหนดหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่ายให้เกิดความชัดเจน เพื่อหลีกเลี่ยงการใช้งานสินทรัพย์ผิดวัตถุประสงค์ หรือโดยไม่มีสิทธิ์

7.2 การจัดการผู้ให้บริการภายนอก

ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการด้านเทคโนโลยีสารสนเทศของหน่วยงานภายนอก โดยต้องประกอบไปด้วยรายละเอียดดังนี้

- การยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท
- ขอบเขต รายละเอียด และระดับการให้บริการ
- เอกสารต่าง ๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้านกายภาพ และด้าน Logical
- เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคง ปลอดภัยสารสนเทศได้ทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความถูกต้องเชื่อถือได้ และการรักษาความพร้อมที่จะให้บริการ
- ข้อตกลงการเชื่อมโยงระบบเครือข่ายของหน่วยงานภายนอก
- ข้อมูลที่หน่วยงานภายนอกสามารถเข้าถึงได้ ขั้นตอนและวิธีการร้องขอข้อมูลของบริษัท กรณีต้องการข้อมูลเพิ่มเติม

- สัญญาในการไม่เปิดเผยข้อมูลของบริษัท
- การยืมหรือการร้องขอใช้อุปกรณ์ของบริษัท
- ข้อกำหนดทางด้านกฎหมาย เช่น ความลับส่วนบุคคล และการป้องกันข้อมูล
- ให้องค์กรสารสนเทศทบทวนและตรวจสอบบริการจาก ผู้ให้บริการภายนอกตามข้อตกลงที่กำหนด
- ให้องค์กรสารสนเทศเป็นผู้รับผิดชอบในการบริหารจัดการการเปลี่ยนแปลงการให้บริการจากผู้ให้บริการภายนอก

7.3 การวางแผนและการยอมรับระบบสารสนเทศ

หน่วยงานสารสนเทศต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถทรัพยากร ปัจจุบันอย่างสม่ำเสมอตามความเหมาะสมของทรัพยากรชนิดต่าง ๆ โดยปฏิบัติตามเอกสาร คู่มือการจัดการขีดความสามารถ

หน่วยงานสารสนเทศต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรสารสนเทศในอนาคต (อาทิ ความต้องการใน 1 ปีที่จะถึง อาทิ CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

หน่วยงานสารสนเทศ ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือ ทรัพยากรสารสนเทศอื่นๆ ก่อนการใช้งาน รวมทั้งต้องทำการทดสอบก่อนที่จะตรวจรับระบบนั้นด้วย โดยปฏิบัติตามเอกสารคู่มือการจัดการการยอมรับระบบ

7.4 การควบคุม และป้องกันการใช้งานระบบ และอุปกรณ์ เคลื่อนที่ผลิตภัณฑ์ประสงค์

เครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดที่ได้รับการอนุมัติจากหน่วยงานสารสนเทศและต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง โดยปฏิบัติตามเอกสารคู่มือการจัดการควบคุมซอฟต์แวร์ไม่ประสงค์ดี

เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊กทุกเครื่องจะต้องได้รับการปรับปรุงข้อมูลความปลอดภัยและอัปเดตล่าสุดจากระบบที่ให้บริการการป้องกันไวรัสอยู่เสมอ

ห้ามเจ้าหน้าที่ทำการดาวน์โหลดแฮร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ตโดยปราศจากการอนุมัติจากหน่วยงานสารสนเทศ หลังจากการอนุมัติแล้วเจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัสก่อนการใช้งาน

ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล สำเนาจากแผ่นดิสก์ หรือไฟล์ แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัสก่อนการใช้งาน

ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมัลแวร์ใด ๆ ตัวอย่าง ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมลบอมบ์ เข้าสู่ระบบคอมพิวเตอร์ของบริษัท

ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายของบริษัทได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้นนอกจากนี้ผู้ใช้งาน ต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสของบริษัทก่อนเปิดใช้งานเสมอ

เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่ต้องจำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดี มีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านั้น

ห้ามผู้ใช้งานติดตั้งโปรแกรมชนิดเคลื่อนที่ได้ อาทิ ActiveCode ต่างๆ (เช่น Java, Active X) จากแหล่งที่ไม่น่าเชื่อถือในอินเทอร์เน็ต

7.5 นโยบายการสำรองข้อมูล

หน่วยงานสารสนเทศ ต้องกำหนดความถี่ในการทำการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูล และการยอมรับความเสี่ยงที่กำหนดโดยเจ้าของข้อมูล หรือระบบ โดยปฏิบัติตามเอกสารคู่มือการจัดการสำรองข้อมูลสารสนเทศ

หน่วยงานสารสนเทศ ต้องจัดให้มีการดูแลรักษาอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพสามารถใช้งานได้ตลอดเวลา

หน่วยงานสารสนเทศ ต้องจัดให้มีการควบคุมการเข้าถึงทางกายภาพของสถานที่ที่จัดเก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกัน

หน่วยงานสารสนเทศ ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูลและการเรียกคืนข้อมูลในแต่ละครั้ง ข้อมูลสำรองต้องได้รับการทดสอบเป็นระยะๆ เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้สามารถกู้ข้อมูลกลับมาได้อย่างสมบูรณ์

หน่วยงานสารสนเทศ ต้องจัดให้มีการจัดเก็บข้อมูลสำรองอย่างน้อย 2 แห่ง โดยแยกสถานที่จัดเก็บข้อมูลสำรองออกจากสถานที่หลักและมีความมั่นคงปลอดภัย เพื่รองรับการกู้คืนระบบในกรณีเกิดเหตุฉุกเฉิน

7.6 การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย

หน่วยงานสารสนเทศ ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมี เหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

หน่วยงานสารสนเทศ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญ และแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่ายบริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสม และต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของบริษัทด้วย

ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Package Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

หน่วยงานสารสนเทศ ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของบริษัท และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะ และติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น

ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบ เครือข่ายของบริษัท โดยไม่ได้รับอนุญาตจากหน่วยงานสารสนเทศ

ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัทโดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่าง Router, Switch, Hub และ Wireless Access Point โดยไม่ได้รับอนุญาตเด็ดขาด

ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของบริษัททำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในบริษัทโดยเด็ดขาด

7.7 การแลกเปลี่ยนข้อมูลสารสนเทศ

ให้หน่วยงานสารสนเทศกำหนดวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือ ซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย

ให้หน่วยงานสารสนเทศกำหนดวิธีการป้องกันการเข้าถึงข้อมูล อิเล็กทรอนิกส์รวม ถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

ให้หน่วยงานสารสนเทศกำหนดนโยบายและขั้นตอนการป้องกันการแลกเปลี่ยนข้อมูลระหว่างบริษัท

7.8 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย

ให้หน่วยงานสารสนเทศทำการบันทึกกิจกรรม (Audit Logging) การใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

ให้หน่วยงานสารสนเทศตรวจสอบการใช้งานสินทรัพย์สารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

ให้หน่วยงานสารสนเทศบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator And Operator Logs)

ให้หน่วยงานสารสนเทศบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging) ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศวิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

ให้หน่วยงานสารสนเทศตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในหน่วยงานให้ตรงกัน (Clock Synchronization) โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ของบริษัทถูกบุกรุก

หมวด 8

การควบคุมการเข้าถึง

8.1 การควบคุมการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศ

- หน่วยงานสารสนเทศ ร่วมกับผู้รับผิดชอบข้อมูลและระบบสารสนเทศของแต่ละหน่วยงานเป็นผู้กำหนดสิทธิ์มาตรฐานการเข้าถึงข้อมูล และระบบสารสนเทศหลักของบริษัท
- หน่วยงานสารสนเทศ ต้องจัดให้มีระบบควบคุมในการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- หน่วยงานสารสนเทศ ต้องกำหนดการควบคุมการเข้าถึงระบบให้มีความมั่นคงปลอดภัย ดังนี้
 - กำหนดให้ระบบให้บริการปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดเกิน 3 ครั้ง
 - กำหนดให้ระบบควบคุมดูแลให้ผู้ใช้งานระบบงานหลักของบริษัทเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
- กำหนดให้หน่วยงานสารสนเทศเป็นผู้ดูแลระบบของบริษัททั้งหมด มีสิทธิ์ในแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้
- หน่วยงานสารสนเทศ ต้องมีการเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ
- หน่วยงานสารสนเทศ ต้องจัดให้มีการควบคุมการกำหนดสิทธิ์และการใช้สิทธิ์ ดังนี้
 - บัญชีผู้ใช้งานในระดับพิเศษ เช่น Root หรือ Administrator ของระบบงานสารสนเทศทุกระบบ ต้องได้รับการพิจารณาอนุญาตให้แก่อุปกรณ์ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาการเข้าถึงอย่างเหมาะสมกับการทำงานนั้น
 - บัญชีผู้ใช้งานในระดับพิเศษ เช่น Root หรือ Administrator สำหรับเข้าถึง Server, Database, Cloud, Co-locatoin ต้องได้รับการพิจารณาอนุญาตให้แก่อุปกรณ์ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาการเข้าถึงอย่างเหมาะสมกับการทำงานนั้น
 - บัญชีผู้ใช้งานสำหรับเข้าถึง Database ต้องได้รับการพิจารณาอนุญาตให้แก่อุปกรณ์ใช้งานตามความจำเป็น

- หน่วยงานสารสนเทศต้องวางมาตรการการเข้าถึงข้อมูลทั้งทางด้าน Hardware และ Software เพื่อให้เกิดความปลอดภัย ดังนี้

1. มาตรการด้าน Hardware

1.1 กำหนดมาตรฐานสำหรับอุปกรณ์ที่ใช้กับสำนักงานโครงการ

- กำหนดให้เครื่องถ่ายเอกสารที่ติดตั้ง ณ สำนักงานโครงการต้องรองรับการ Scan เอกสารขึ้นไปเก็บไว้บน Cloud ได้ทันที เพื่อลดขั้นตอนการทำงานและลดความเสี่ยง ข้อมูลรั่วไหล จากกรณีที่ข้อมูลถูกเก็บไว้ที่คอมพิวเตอร์ที่สำนักงานก่อน Copy ข้อมูลไปส่วนกลาง

1.2 กำหนดมาตรการสำหรับการใช้เครื่องคอมพิวเตอร์ลูกข่าย

- กำหนดให้ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ลูกข่าย จัดเก็บบน Cloud MS365
- กำหนดมาตรการทำลายข้อมูลบนเครื่องคอมพิวเตอร์เข้ามดอายุก่อนส่งคืน
- กำหนดมาตรการทำลายข้อมูลบนเครื่องคอมพิวเตอร์ทรัพย์สินก่อนตัดจำหน่าย

1.3 กำหนดมาตรการการเข้าถึง Server และ Database

- กำหนดให้มีการทบทวนสิทธิ์ในการเข้าถึงห้อง Data Center, Co-location อย่างน้อยปีละ 1 ครั้ง
- กำหนดให้มีการทบทวนสิทธิ์ในการเข้าถึงระบบ Server, Cloud, Database และ User Admin ของแต่ละระบบ อย่างน้อยปีละ 2 ครั้ง
- กำหนดให้มีการเก็บบันทึก Log การเข้าถึง Database และ Server อย่างน้อย 30 วัน และการเข้าถึงให้ใช้ Username ของผู้ใช้งานเท่านั้น

2. มาตรการด้าน Software

2.1 แกะไขโปรแกรมที่แสดงผลข้อมูลส่วนบุคคลผ่านเว็บเบราว์เซอร์ ไม่ให้สามารถ Copy ข้อมูลส่วนบุคคลจากหน้าเว็บเพจได้

2.2 กำหนดให้มีการใช้ Software เพื่อจัดเก็บเอกสารไว้ที่ส่วนกลาง (Document Center) เพื่อให้ง่ายต่อการควบคุม ไฟล์เอกสารไม่เก็บกระจายหลายที่ กำหนดสิทธิ์การเข้าถึงได้ครอบคลุม มีระบบสำรองข้อมูล สะดวกต่อการใช้งานได้ทุกที่ทุกเวลา

8.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน

- ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์ แยกตามหน้าที่ที่รับผิดชอบด้วย
- ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-On เข้าสู่ระบบสารสนเทศ
- หน่วยงานสารสนเทศต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัยอยู่เสมอ
- หน่วยงานสารสนเทศต้องตรวจสอบสิทธิ์รายชื่อพนักงานเข้าใหม่และลาออกไตรมาสละ 1 ครั้ง
- หน่วยงานสารสนเทศร่วมกับผู้รับผิดชอบข้อมูลและระบบสารสนเทศของแต่ละสายงานทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง
- หน่วยงานสารสนเทศต้องเก็บบันทึกข้อมูล Log การเข้าใช้งานอินเทอร์เน็ตอย่างน้อย 90 วัน (ตามพรบ.คอมพิวเตอร์)

8.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน

- ผู้รับผิดชอบข้อมูลระบบสารสนเทศของแต่ละหน่วยงาน ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ
- ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงระบบสารสนเทศของบริษัท การกำหนดการเปลี่ยนแปลง และการยกเลิกรหัสผ่าน และการจัดการควบคุมการใช้รหัสผ่านกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุดต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
 - ควรได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาและผู้ดูแลระบบของส่วนงานนั้นๆ
 - ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
 - ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
 - รหัสผ่านต้องได้รับการเปลี่ยนเมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอ
 - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน
- รหัสผ่านถือเป็นข้อมูลลับ และเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านอย่างมั่นคงปลอดภัย ห้ามใช้บัญชีผู้ใช้งานร่วมกัน หรือให้ผู้อื่นเข้าใช้งานบัญชีผู้ใช้งานของตนโดยเด็ดขาด

- ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งาน และรหัสผ่านของตนทั้งหมด หากผู้ใช้งานสงสัยว่าบัญชีผู้ใช้งาน หรือรหัสผ่านของตนถูกล้วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อหน่วยงานสารสนเทศและทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที
- ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนเองรวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้ให้มีความมั่นคงปลอดภัยอย่างสม่ำเสมอ
- ตามช่วง ระยะเวลาที่กำหนดไว้ในเอกสารขั้นตอนการปฏิบัติงานมาตรฐานการใช้รหัสผ่าน
- การ Reset รหัสผ่าน ต้องผ่านกระบวนการมาตรฐานของบริษัทเท่านั้น เพื่อให้มั่นใจว่าตรงกับบัญชีผู้ใช้งานที่ต้องการ Reset รหัสผ่านจริง อีกทั้งเจ้าหน้าที่ ที่ดูแลระบบมีสิทธิ์ในการขอข้อมูล และพิสูจน์ตัวตนของผู้ใช้งานตามความเหมาะสม
- ในทางกลับกัน ผู้ใช้งานอาจได้รับการร้องขอจากหน่วยงานสารสนเทศให้ทำการเปลี่ยนรหัสผ่านใหม่ ในกรณีที่รหัสผ่านของผู้ใช้งานไม่มีความมั่นคงปลอดภัยสามารถถูกคาดเดา หรือถูกล้วงละเมิดได้ง่าย ทั้งนี้ผู้ใช้งานต้องตรวจสอบความถูกต้องของแหล่งที่มาของคำร้องขอดังกล่าวด้วย เพื่อให้มั่นใจว่าการร้องขอนั้นไม่ได้เป็นการหลอกลวง
- ต้องกำหนดการป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ดูแลและเจ้าหน้าที่ต้องกำหนดการควบคุมเอกสารข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ ไม่ให้มีข้อมูลสำคัญปรากฏในขณะไม่ได้ใช้งาน

8.4 การควบคุมการเข้าถึงเครือข่าย

- หน่วยงานสารสนเทศต้องจัดทำแนวทาง/นโยบายควบคุมการเข้าถึง เครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
- หน่วยงานสารสนเทศต้องมีการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ และต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
- หน่วยงานสารสนเทศต้องจัดแบ่งระบบเครือข่ายตามกลุ่มของบริการระบบ เทคโนโลยีสารสนเทศ ที่มีการใช้งานแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน

(Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับ ขอบเขตของเครือข่ายภายใน และเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่ เสมอ

- หน่วยงานสารสนเทศต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

8.5 การใช้งานคอมพิวเตอร์ประเภทพกพา โทรศัพท์มือถือ และอุปกรณ์บันทึกข้อมูล

- พนักงานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, Palmtops, Laptop) และอุปกรณ์สื่อสารอื่นๆ เมื่อปฏิบัติงานอยู่นอกสถานที่
 - ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
 - ต้องใส่รหัสผ่านป้องกันข้อมูลที่สำคัญ
- กรณีพนักงานใช้โทรศัพท์มือถือ Tablet ที่เป็นของส่วนตัวเชื่อมต่อเครือข่ายของบริษัทจะต้องดำเนินการขออนุญาตตามขั้นตอนของหน่วยงานสารสนเทศก่อน
- ห้ามพนักงานใช้อุปกรณ์บันทึกข้อมูลใดๆ ที่เป็นของส่วนตัวทำการคัดลอกข้อมูลของบริษัท เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน และผู้รับผิดชอบข้อมูลและระบบสารสนเทศของหน่วยงานนั้นๆ

หมวด 9

การจัดการ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

9.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ

- หน่วยงานสารสนเทศต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน
- หน่วยงานสารสนเทศจะต้องทำการวิเคราะห์ระบบเทคโนโลยี สารสนเทศว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้
 - มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง
 - มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

9.2 การประเมินผลระบบสารสนเทศ

- ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการประมวลผลข้อมูลสารสนเทศ (Checks And Controls) ว่ามีข้อผิดพลาดหรือไม่
- ผู้พัฒนาระบบสารสนเทศต้องมีวิธีการตรวจสอบการส่งข้อมูลในระบบสารสนเทศ เพื่อให้แน่ใจว่าข้อมูลในระบบสารสนเทศมีความปลอดภัยและมีความถูกต้องสมบูรณ์
- ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการตรวจสอบ ทดสอบและประเมินผลเพื่อให้มั่นใจว่าระบบสามารถใช้ได้จริงและมีผลลัพธ์ที่ถูกต้อง
- หน่วยงานที่มีการส่งข้อมูลส่วนบุคคลให้กับบุคคลภายนอกดำเนินการประมวลผลข้อมูล จะต้องจัดทำบันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคลให้รองรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

9.3 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ

- ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบรารี ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหาเกี่ยวกับเครื่องที่ให้บริการอยู่

- ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบจะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที
- ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการ

9.4 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ

- ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว อาทิ
 - คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ
 - ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
 - เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้ขอ
- เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลงซอฟต์แวร์ต่าง ๆ ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัยในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

9.5 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

หน่วยงานสารสนเทศต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน และประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับ เพื่อลดความเสี่ยงดังกล่าว

หมวด 10

การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

กำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัท การบริหารจัดการ และการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ

กำหนดให้มีการทดสอบกระบวนการในการสร้างความต่อเนื่องให้กับการปฏิบัติงานของบริษัทอย่างสม่ำเสมอ

หมวด 11

การปฏิบัติตามข้อกำหนด

11.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย

หน่วยงานสารสนเทศต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศของหน่วยงาน

เจ้าหน้าที่ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ ที่กำหนดขึ้นอย่างเคร่งครัด โดยมี รายการดังต่อไปนี้เป็นอย่างน้อย

- นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.บ. ลิขสิทธิ์
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทถือเป็นทรัพย์สิน ของ บริษัท ทั้งนี้บริษัทสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้ เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่ จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศของบริษัทขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และ ระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามนโยบายต่าง ๆ กำหนดไว้ ตลอดจนการ เข้าถึง ทบทวน และตรวจสอบอีเมลล์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

อย่างไรก็ตามการตรวจสอบดังกล่าวจะดำเนินการต่อเมื่อมีความจำเป็นเท่านั้น และจะไม่เปิดเผย ข้อมูลใดๆ ของผู้ใช้งาน เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบังคับของกฎหมาย หรือด้วยความ ยินยอมจากผู้ใช้งานเท่านั้น

ห้ามเจ้าหน้าที่ทุกคนใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัท กระทำการใดๆ ที่ ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งาน และต้องระมัดระวังที่จะไม่ละเมิด ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่าง เคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การเก็บหลักฐานแสดง ความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศ ของบริษัทโดย เด็ดขาด

ต้องมีการวางระบบให้พร้อมสำหรับเจ้าของข้อมูลในการขอใช้สิทธิ์ดังต่อไปนี้ ให้แล้วเสร็จภายใน 30 วัน หลังรับเรื่อง

1. ขอดูและขอสำเนาข้อมูลส่วนบุคคลของลูกค้าได้
2. สิทธิในการขอรับหรือขอส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปบุคคลภายนอก
3. ขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
4. ขอให้ลบหรือทำลายข้อมูลส่วนบุคคล (เราอาจจะใช้วิธีการทำให้ข้อมูลนั้นระบุตัวตนไม่ได้)
5. ขอให้ระงับการใช้ข้อมูลส่วนบุคคล

6. สิทธิในการคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูล
7. สิทธิในการขอถอนความยินยอม ที่เคยยินยอมไว้
8. สิทธิในการร้องเรียนต่อ DPO

และวางระบบการจัดเก็บความยินยอมจากลูกค้าให้สามารถตรวจสอบและพร้อมนำมาใช้งานได้

11.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัย

หน่วยงานสารสนเทศต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้

หน่วยงานสารสนเทศต้องตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือ ให้บริการอยู่ แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การ ตรวจสอบว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning)

11.3 การพิจารณาการตรวจสอบระบบสารสนเทศ

หน่วยงานสารสนเทศต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบ ที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

หน่วยเทคโนโลยีสารสนเทศต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น

แผนรองรับสถานการณ์ฉุกเฉิน

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร ฝ่ายสารสนเทศได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลขององค์กร ซึ่งอาจมีปัจจัยจากภายในและปัจจัยภายนอก อันมีเหตุให้ระบบขององค์กรหยุดชะงักหรือไม่สามารถดำเนินการได้ ดังนั้นจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินและเหตุภัยพิบัติ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการปฏิบัติและแก้ไขปัญหาที่เกิดขึ้น ดังนี้

1. การประเมินความรุนแรงของสถานการณ์

- 1.1 เกิดจากสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้ง
- 1.2 เกิดจากภัยธรรมชาติ ได้แก่ ภัยพิบัติ, อัคคีภัย, อุทกภัย, แผ่นดินไหว ฯลฯ

2. แนวทางการป้องกันและแนวทางปฏิบัติงานกรณีเกิดเหตุฉุกเฉินเบื้องต้น

ฝ่ายสารสนเทศได้จัดทำ “คู่มือการปฏิบัติงานกรณีเกิดเหตุฉุกเฉิน” เพื่อให้เจ้าหน้าที่ทุกคนทราบและเป็นแนวทางการปฏิบัติตัวอย่างเคร่งครัด รวมทั้งมีการจัดอบรมซ้อมหนีไฟเพื่อเป็นแนวทางการปฏิบัติตามแผนด้วย หากเมื่อเกิดเหตุการณ์ฉุกเฉินจะดำเนินการประสานงานได้อย่างถูกต้อง เพื่อพิจารณาและประกาศใช้แผนต่อไป

3. การเตรียมความพร้อมเพื่อรองรับกรณีเกิดเหตุฉุกเฉิน

3.1 สถานที่ตั้งสำรองกรณีเกิดเหตุฉุกเฉิน

- 3.1.1 สถานที่ใช้เป็น Data Center สำรอง
 - Co-Location หรือ Private Cloud

- 3.1.2 สถานที่สำหรับใช้เป็นสำนักงานสำรอง เลือกตามความเหมาะสม ดังนี้
 - ศูนย์อบรม P.S.T City Home
 - สำนักงานขยายโครงการ

3.2 บริษัทผู้ให้บริการเช่าอุปกรณ์กรณีเกิดเหตุฉุกเฉิน

- 3.2.1 บริษัท คอมเทรตติ้ง จำกัด (คุณเอมมี 083-007-5158)
- 3.2.2 บริษัท ไซเฟอร์เมต จำกัด (คุณเกด 062-875-9969)

3.3 อุปกรณ์ที่ต้องใช้งานสำหรับการกู้คืนข้อมูลระบบหลัก RMS กรณีเกิดเหตุฉุกเฉิน

- 3.3.1 SERVER สำหรับระบบ RMS, AD, Terminal 1 เครื่อง
- 3.3.2 COMPUTER DESKTOP สำหรับพนักงาน 5 เครื่อง
- 3.3.3 ระบบสำรองไฟฟ้า 1 เครื่อง

3.3.4 Printer Network

3.3.5 NETWORK SWITCH และสายแลน

4. กำหนดผู้รับผิดชอบกรณีเกิดเหตุฉุกเฉิน

4.1 รับผิดชอบขนย้ายอุปกรณ์ Server, Network และ Firewall ที่สามารถเคลื่อนย้ายได้ไปยังจุดรวมพลนอกอาคาร

- System Administrator ผู้ดูแลระบบที่เกี่ยวข้อง

4.2 รับผิดชอบประสานงานจัดหา HARDWARE / SOFTWARE ตามแผนฉุกเฉิน

- IT Support และ HW Support ที่เกี่ยวข้อง

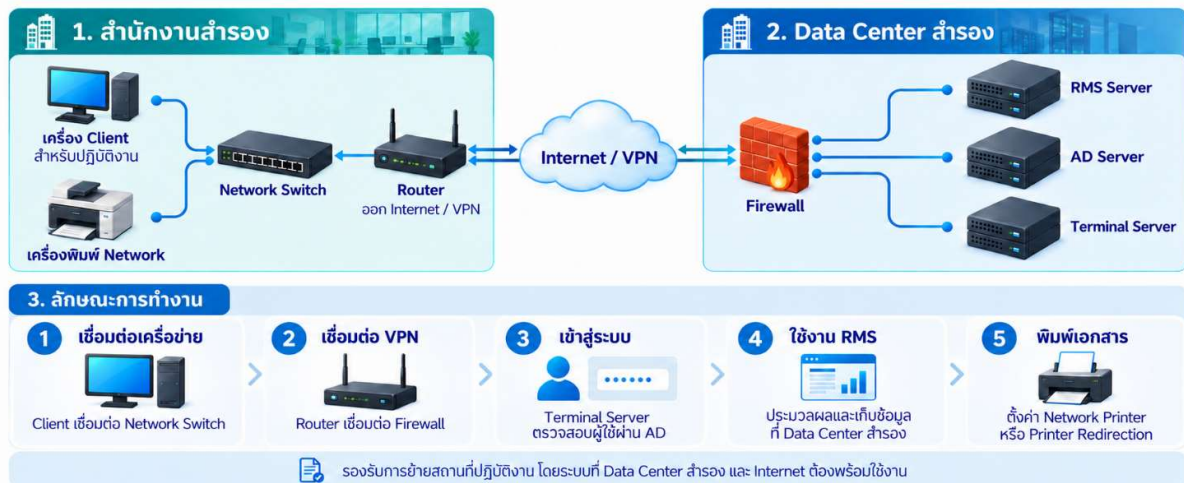
4.4 ผู้ประเมินสถานการณ์

- ผู้อำนวยการสำนักสารสนเทศ
- รองประธานเจ้าหน้าที่บริหาร, ประธานเจ้าหน้าที่บริหาร

4.5 ผู้อนุมัติใช้แผนฉุกเฉิน

- ประธานเจ้าหน้าที่บริหาร

5. Diagram รองรับการกู้คืนระบบหลักกรณีเกิดเหตุฉุกเฉิน



1.สำนักงานสำรอง	2.Data Center สำรอง	3.ลักษณะการทำงาน
สถานที่ที่ให้หน่วยงานต่างๆ เข้าปฏิบัติงานชั่วคราว โดยมีการเตรียมความพร้อมระบบงาน และอุปกรณ์เท่าที่จำเป็น	Co-Location/Private Cloud ที่ใช้เป็น Data Center สำรอง เพื่อกู้คืนข้อมูลระบบ RMS และเชื่อมต่อกับสำนักงานสำรอง	ผู้ใช้งานจากสำนักงานสำรองเชื่อมต่อเครือข่ายผ่าน VPN ไปยัง Data Center สำรอง และเปิดใช้ระบบ RMS ตามปกติ

6. ขั้นตอนดำเนินการกู้คืนระบบกรณีเกิดเหตุฉุกเฉิน

ขั้นตอน	การดำเนินการ	ระยะเวลา
1	สำนักงานสำรอง ดำเนินการ ดังนี้ - ติดตั้งอุปกรณ์เชื่อมต่อ Network Switch, Router, UPS, สาย LAN - ติดตั้งเครื่องคอมพิวเตอร์ พรินเตอร์ และซอฟต์แวร์ที่จำเป็น สำหรับหน่วยงานต่างๆ อย่างน้อย 5 ชุด	3-6 ชม.
2	Data Center สำรอง ดำเนินการ ดังนี้ - ติดตั้ง Server สำหรับการกู้คืนข้อมูลระบบ RMS - ติดตั้ง Server AD สำหรับการควบคุมการ Authen ระบบงาน - ติดตั้ง Terminal Server, VPN และ Firewall เพื่อให้ Client เชื่อมต่อ - เตรียมข้อมูลสำรองชุดล่าสุดของระบบ RMS - ทำการกู้คืนข้อมูลระบบ RMS จากข้อมูลสำรองชุดล่าสุด - ตรวจสอบการตั้งค่าของระบบและการเชื่อมต่อเครือข่าย - ทดสอบการใช้งานระบบ และตรวจสอบความถูกต้องของข้อมูล	3-6 ชม.
3	ทดสอบการใช้งาน ณ สำนักงานสำรอง - กำหนดตัวแทนของแต่ละหน่วยงานเพื่อทดสอบการใช้งานแยกตามระบบ เช่น งานขาย,เช่า,บัญชี,การเงิน - ผู้ทดสอบ ทดสอบระบบโดยใช้ข้อมูลจริง - ผู้ทดสอบระบบสรุปผลการทดสอบ - กรณีผู้ทดสอบพบปัญหาจากการทดสอบให้แจ้ง MIS เพื่อดำเนินการแก้ไข จนกว่าจะใช้งานได้ปกติ - กรณีผู้ทดสอบไม่พบปัญหาให้แจ้งต่อผู้บังคับบัญชา และ MIS รับทราบ เพื่อประกาศเปิดใช้งานระบบ	1-2 ชม.

7. การติดตามและรายงานผล

รายงานผลการปฏิบัติงานตามขั้นตอนการกู้คืนระบบต่อผู้บริหารสูงสุด เพื่อพิจารณาและดำเนินการต่อไป

แนวปฏิบัติเมื่อเกิดเหตุฉุกเฉิน

แนวทางการดำเนินงานเมื่อเกิดเหตุฉุกเฉิน

1. กรณีสถานการณ์ไฟไหม้ในช่วงเวลาทำงาน

ขั้นตอนการดำเนินการ

- 1.1 เมื่อได้ยินเสียงตามสายหรือสัญญาณเตือนภัยดัง ให้เจ้าหน้าที่ดูแล Backup ส่งสำรองข้อมูลทันที
- 1.2 ผู้จัดการสำนักสารสนเทศวิเคราะห์จุดเกิดเหตุว่ามีผลกระทบกับห้อง Server หรือไม่
 - 1.2.1 กรณีจุดเกิดเหตุมีผลกระทบกับ Server ให้เจ้าหน้าที่ MIS ดำเนินการดับเพลิงขั้นต้นได้ หากไม่สามารถควบคุมเพลิงได้ ให้ส่งอพยพทันที และรายงานสถานการณ์ ตามลำดับบังคับบัญชา
 - 1.2.2 กรณีจุดเกิดเหตุไม่มีผลกระทบ Server ให้เจ้าหน้าที่ MIS ดำเนินการตามมาตรการหนีไฟ
- 1.3 เมื่ออพยพถึง ณ จุดรวมพล เจ้าหน้าที่ดูแล Backup ตรวจสอบผลการส่ง Backup และรายงานสถานะข้อมูลที่สามารถ Backup ได้ล่าสุดแก่ ผู้จัดการสำนักสารสนเทศ
- 1.4 ผู้จัดการสำนักสารสนเทศรายงานสถานการณ์ให้ผู้อำนวยการสำนักสารสนเทศรับทราบ

2. กรณีสถานการณ์ไฟไหม้นอกช่วงนอกเวลาทำงาน

ขั้นตอนการดำเนินการ

- 2.1 เมื่อเกิดเหตุฉุกเฉิน ศูนย์รับแจ้งเหตุ (EOC) ต้องโทรแจ้งตามรายชื่อ MIS ผู้เกี่ยวข้อง
- 2.2 ให้เจ้าหน้าที่ดูแล Backup ทำการ Remote ส่งสำรองข้อมูลทันที
- 2.3 ทำการตรวจสอบความพร้อมและความถูกต้องของข้อมูลระบบ Backup DR Site และรายงานสถานะข้อมูลที่สามารถ Backup ได้ล่าสุดแก่ ผู้จัดการสำนักสารสนเทศ
- 2.4 เจ้าหน้าที่ MIS ผู้เกี่ยวข้องร่วมประเมินสถานการณ์เพื่อแจ้งผู้จัดการสำนักสารสนเทศและรายงานสถานการณ์ให้ผู้อำนวยการสำนักสารสนเทศรับทราบ

แนวทางการกู้คืนหลังเกิดเหตุฉุกเฉิน

หลังเกิดเหตุ เจ้าหน้าที่ดูแลระบบ ที่รับผิดชอบให้เข้าสำรวจห้อง Server ว่าสามารถใช้งานต่อไปได้ หรือไม่

1. กรณี ห้อง Server เดิมยังสามารถใช้งานได้

ขั้นตอนการดำเนินการ

- 1.1 สำรวจความเสียหาย ที่เกิดขึ้น และสรุปอุปกรณ์ที่เสียหาย
- 1.2 จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
- 1.3 เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

- 1.4 ทดสอบการใช้งาน
- 1.5 หากไม่สามารถใช้งานได้ ให้ Recovery System (Clone Server)
- 1.6 Restore DATA จาก Backup หรือ DR Site ให้ได้ข้อมูล Update ล่าสุดที่มี
- 1.7 ทดสอบการใช้งาน และตรวจสอบข้อมูล
- 1.8 ผู้จัดการสำนักสารสนเทศรายงานสถานการณ์ให้ผู้อำนวยการสำนักสารสนเทศรับทราบ

2. กรณี ห้องServer เดิมไม่สามารถใช้งานได้

ขั้นตอนการดำเนินการ

- 2.1 จัดหาสถานที่ติดตั้ง Server ใหม่
- 2.2 สำรวจความต้องการใช้อุปกรณ์อะไรบ้าง เช่น Server (รุ่น / Spec ไหน), Switch ที่ต้องใช้งาน
- 2.3 ขออนุมัติจัดหาอุปกรณ์ใหม่หรือทดแทนตามที่ต้องใช้งาน
- 2.4 ติดตั้ง Server ใหม่ และ Recovery System (Clone Server)
- 2.5 Restore DATA จาก Backup หรือ DR Site ให้ได้ข้อมูล Update ล่าสุดที่มี
- 2.6 ทดสอบการใช้งาน และตรวจสอบข้อมูล
- 2.7 ผู้จัดการสำนักสารสนเทศรายงานสถานการณ์ให้ผู้อำนวยการสำนักสารสนเทศรับทราบ

ข้อกำหนด

1. กำหนดให้มีการซ้อมแผนฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง (พร้อมกับการซ้อมหนีไฟของอาคาร)
2. แจ้งแผนการดำเนินงานให้กับผู้เกี่ยวข้องรับทราบ
3. ในกรณีเกิดเหตุการณ์ฉุกเฉิน ต้องมีการบันทึกรายละเอียดทุกครั้ง(สาเหตุ,ปัญหา,แนวทางการแก้ไข)

หมายเลขติดต่อผู้เกี่ยวข้อง

1. คุณสุวัฒนา แซ่ตั้ง	ผู้ช่วยกรรมการผู้จัดการ	เบอร์ 081-802-4028
2. คุณพิระวุธ ผาสุข	ผู้จัดการสำนักสารสนเทศ	เบอร์ 093-491-5149
3. คุณเมธาสีทธิ์ ศรีไชยกิจ	ผู้จัดการสำนักสารสนเทศ	เบอร์ 092-254-7197
4. คุณไชยวัฒน์ นิลทอง	Lead System Administrator	เบอร์ 081-756-3171
5. คุณนิกรณ ศรีธรรม	Lead IT Support	เบอร์ 094-252-3636
6. คุณเจตณรงค์ จันทะคาด	Junior System Administrator	เบอร์ 090-672-2752
7. คุณภากร ศรีพยัคฆ์	HW Support	เบอร์ 089-105-2502

แนวปฏิบัติในการใช้งานระบบคอมพิวเตอร์ และอินเทอร์เน็ต

1. การใช้งานระบบคอมพิวเตอร์

- 1.1 บริษัทดำเนินกิจการภายใต้กฎหมายไทย ดังนั้นการใช้งานระบบคอมพิวเตอร์และการใช้งานอินเทอร์เน็ต ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง
- 1.2 บริษัทไม่สนับสนุน หรือยินยอมให้พนักงานกระทำผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายประกอบอื่นๆที่เกี่ยวข้อง
- 1.3 บริษัทจัดให้มีชื่อผู้ใช้ (USERNAME) และรหัสผ่าน(PASSWORD) ให้กับพนักงานที่มีหน้าที่เกี่ยวข้องกับการใช้งานระบบคอมพิวเตอร์และการใช้งานอินเทอร์เน็ต เป็นรายบุคคล และมีกฎในการใช้งานรหัสผ่าน ทั้งนี้เพื่อความปลอดภัยของระบบโดยรวม
- 1.4 รหัสผ่าน (PASSWORD) ของพนักงานถือเป็นทรัพย์สินของบริษัท และบริษัทกำหนดให้ใช้เป็นรายบุคคล พนักงานมีหน้าที่ในการป้องกันรหัสผ่านของตนเองอย่างเคร่งครัด ไม่อนุญาตให้มีการแจ้งรหัสผ่านให้กับบุคคลอื่นทราบไม่ว่ากรณีใดๆ และ
- 1.5 ระบบคอมพิวเตอร์, เครื่องคอมพิวเตอร์พีซี, โน้ตบุ๊ก, สมาร์ทโฟน, แท็บเล็ต และอุปกรณ์ต่างๆ ที่บริษัทจัดหา มาให้เพื่อใช้ในการทำงานที่เกี่ยวข้องกับกิจการของบริษัทเท่านั้น ไม่อนุญาตให้นำไปใช้ส่วนตัว หรือในกิจการที่ไม่เกี่ยวข้องกับบริษัท
- 1.6 ไม่อนุญาตให้นำระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์พีซี, โน้ตบุ๊ก ที่ไม่ใช่ของบริษัทเข้ามาใช้ในสถานที่ทำงานของบริษัท ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษร จากกรรมการผู้จัดการเท่านั้น
- 1.7 ไม่อนุญาตให้นำ สมาร์ทโฟน, แท็บเล็ต และอุปกรณ์ต่อพ่วงต่างๆ ที่เป็นของส่วนตัวเชื่อมต่อเข้ากับคอมพิวเตอร์พีซี หรือโน้ตบุ๊กของบริษัท
- 1.8 การเข้าใช้งานระบบคอมพิวเตอร์ ,อินเทอร์เน็ต และเครือข่ายไร้สาย (Wifi) ของบริษัทจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานคอมพิวเตอร์ กรณีต้องการใช้งานนอกเหนือจากข้อกำหนดจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาสูงสุดโดยตรง
- 1.9 สมาร์ทโฟน, แท็บเล็ต ที่เป็นของส่วนตัวพนักงาน อนุญาตให้เชื่อมต่อเครือข่ายไร้สาย (Wifi) ของบริษัทได้ภายใต้ข้อกำหนดเท่านั้น

2. การใช้อีเมล และการติดต่อสื่อสารทางโซเชียล มีเดีย

- 2.1 การส่งข้อมูลใดๆ ให้ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- 2.2 ไม่อนุญาตให้พนักงานใช้อีเมลอื่นที่บริษัทไม่ได้กำหนดให้ใช้ ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาสูงสุดโดยตรง
- 2.3 ห้ามนำข้อมูลของบริษัทที่ยังไม่ได้รับอนุญาตไปเผยแพร่
- 2.4 ห้ามส่งข้อมูลที่เป็นเท็จ ข้อมูลที่ก่อให้เกิดความเสียหายต่อบริษัท หรือบุคคลอื่นๆ
- 2.5 ห้ามส่งรูปหรือข้อความที่เกี่ยวข้องกับเรื่องลามกอนาจาร
- 2.6 ให้ใช้ข้อความสุภาพในการสนทนา หรือการสื่อสารทางโซเชียล มีเดีย
- 2.7 ห้ามส่งต่ออีเมล ที่มีลักษณะเป็นจดหมายลูกโซ่ หรืออีเมลที่ไม่รู้จัก

3. การใช้ อินทราเน็ต และอินเทอร์เน็ตขององค์กร

- 3.1 ห้ามพนักงาน นำเข้าข้อมูลใดๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- 3.2 ห้ามมีไวรัส หรือชุดคำสั่งไม่พึงประสงค์
- 3.3 ห้ามพนักงาน คาวานีโหลดข้อมูลใดๆ ที่เข้าข่ายผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

4. การใช้งานซอฟต์แวร์

- 4.1 ให้พนักงานใช้ซอฟต์แวร์ที่บริษัท กำหนดให้ใช้เท่านั้น
- 4.2 บริษัทกำหนดให้พนักงานสามารถใช้ซอฟต์แวร์ต่างๆ ตามความจำเป็นที่ในเบื้องต้น และให้ขออนุญาตใช้เพิ่มเติมได้ตามความจำเป็นโดยให้ผู้บังคับบัญชาโดยตรงเป็นผู้อนุญาตเป็นลายลักษณ์อักษร
- 4.3 ห้ามพนักงานนำซอฟต์แวร์ใด ๆ มาติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท โดยไม่ได้รับความยินยอมจากหน่วยงานคอมพิวเตอร์ และผู้บังคับบัญชาโดยตรง

5. การจัดเก็บข้อมูล และสำรองข้อมูล

- 5.1 บริษัทไม่อนุญาตให้มีการจัดเก็บข้อมูลที่มีความสำคัญไว้บนเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เพราะข้อมูลที่อยู่บนเครื่องคอมพิวเตอร์นั้นๆ จะไม่มีการสำรองข้อมูลใดๆ ทั้งสิ้น
- 5.2 บริษัทกำหนดให้มีการจัดเก็บไฟล์ข้อมูลที่สำคัญไว้ที่ส่วนกลางเท่านั้น โดยกำหนดโดเมนสำหรับจัดเก็บข้อมูลส่วนกลางไว้ดังนี้

- 5.2.1 ไดรฟ์ Sharepoint กำหนดให้เป็นไดรฟ์ส่วนกลางที่ใช้จัดเก็บข้อมูลระดับองค์กร ระดับทีมและระดับฝ่าย เช่น MIS-CENTER กำหนดให้เป็นไดรฟ์ส่วนกลางที่ใช้จัดเก็บข้อมูลร่วมกันในระดับฝ่าย โดยพนักงานในฝ่ายเดียวกันจะได้สิทธิ์ในการใช้ไดรฟ์ Sharepoint ของฝ่าย อัตโนมัติ และจะเห็นข้อมูลของฝ่ายตัวเองเท่านั้น
- 5.2.2 ไดรฟ์ Onedrive ส่วนบุคคล กำหนดให้เป็นไดรฟ์ที่ใช้จัดเก็บข้อมูลส่วนบุคคลโดยพนักงานแต่ละคนจะได้รับสิทธิ์ในการใช้ไดรฟ์ OneDrive โดยอัตโนมัติตามนโยบายที่ทางบริษัทกำหนด และจะเห็นข้อมูลของตัวเองเท่านั้น
- 5.2.3 ไดรฟ์ M: กำหนดให้เป็นไดรฟ์ส่วนกลางที่ใช้จัดเก็บข้อมูลที่ใช้ร่วมกันในระดับองค์กร (อนุญาตให้ใช้งานไปจนกว่าจะอพยพขึ้น Sharepoint) โดยผู้ต้องการวางข้อมูลในไดรฟ์นี้จะต้องให้ผู้จัดการฝ่ายต้นเรื่องทำการขอสิทธิ์ในการสร้างโฟลเดอร์และวางข้อมูลมายังสำนักสารสนเทศเป็นลายลักษณ์อักษร และต่อไปการเข้าถึงข้อมูลในโฟลเดอร์นั้นๆ ผู้จัดการฝ่ายที่เป็นเจ้าของโฟลเดอร์เป็นผู้อนุญาตการเข้าถึงข้อมูลของตนเอง
- 5.3 บริษัทกำหนดให้มีการสำรองข้อมูลเป็นประจำ โดยกำหนดการสำรองข้อมูล ดังนี้
- 5.3.1 ข้อมูลในรูปแบบฐานข้อมูลบนเครื่องแม่ข่ายทุกเครื่อง
- 5.3.2 ข้อมูลในรูปแบบไฟล์ ที่เก็บอยู่บนไดรฟ์กลาง M: เท่านั้น
- 5.3.3 รูปแบบการสำรองข้อมูลจะแบ่งเป็น รายวัน และรายเดือน โดยการสำรองข้อมูลจะถูกจัดเก็บไว้บนระบบสำรองข้อมูลเครื่องแม่ข่ายหลัก DC-Site และจะทำการสำเนาการสำรองข้อมูลไปจัดเก็บไว้บนระบบสำรองข้อมูลเครื่องแม่ข่ายรอง DR-Site ทุกวัน
- 5.3.4 ระบบจะเริ่มสำรองข้อมูลตั้งแต่วันที่ 18.00 น. เป็นต้นไปโดยไล่เรียงตามลำดับความสำคัญ
- 5.4 รายการที่ไม่ได้ทำการสำรองข้อมูล มีดังนี้
- 5.4.1 ข้อมูลที่อยู่บนเครื่องคอมพิวเตอร์ปฏิบัติงาน
- 5.4.2 ข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูลทุกชนิด
- 5.5 การจัดเก็บอุปกรณ์สำรองข้อมูล กำหนดไว้ดังนี้
- 5.5.1 ระบบสำรองข้อมูลเครื่องแม่ข่ายหลัก DC-Site (IN-SITE) สำหรับเก็บสำรองข้อมูลรายวัน และรายเดือน จะจัดเก็บไว้ที่สำนักงานใหญ่ เพื่อความสะดวกรวดเร็วในการเรียกใช้งาน

5.5.2 ระบบสำรองข้อมูลเครื่องแม่ข่ายหลัก DR-Site Co-location (OUT-SITE) สำหรับเก็บสำรองข้อมูลรายวัน และรายเดือน จะจัดเก็บนอกสถานที่ตั้งสำนักงานใหญ่ เพื่อใช้กรณีเกิดเหตุฉุกเฉิน (กำหนดสถานที่จัดเก็บไว้ที่ ศูนย์โทรคมนาคม สาขานนทบุรี (Data Center) ระยะทางห่างจากสำนักงานใหญ่มากกว่า 30 กม.

5.6 การขอกู้คืนข้อมูล

5.6.1 ผู้ที่ขอกู้คืนข้อมูลจะต้องแจ้งความประสงค์เป็นลายลักษณ์อักษร และลงนามอนุมัติให้ดำเนินการโดยผู้จัดการฝ่ายต้นเรื่อง และผู้จัดการสำนักสารสนเทศ

5.6.2 ข้อมูลที่ขอกู้คืนจะต้องอยู่ใคร่ฟที่มีการสำรองข้อมูลเท่านั้น

5.6.3 ข้อมูลที่สร้างใหม่, ลบ หรือแก้ไข ในระหว่างวันก่อนถึงเวลาที่ระบบจะสำรองข้อมูลไม่สามารถกู้คืนได้

6. ระเบียบปฏิบัติของผู้ดูแลระบบคอมพิวเตอร์

6.1 การแบ่งหน้าที่ดูแลระบบคอมพิวเตอร์ของสำนักสารสนเทศ

6.1.1 ผู้ดูแลด้านความปลอดภัยของระบบ ประกอบด้วยเจ้าหน้าที่ในแผนกพัฒนาโครงสร้าง

6.1.2 ผู้ดูแลระบบฐานข้อมูล กำหนดสิทธิ์ให้ไม่เกิน 2 คน และอาจมีการกำหนดสิทธิ์ให้เพิ่มเติมเป็นครั้งคราวขึ้นอยู่กับความจำเป็น โดยผ่านการอนุมัติจากผู้มีอำนาจสูงสุดของสำนักสารสนเทศ

6.1.3 ผู้ดูแลด้านการพัฒนาระบบงาน ประกอบด้วยเจ้าหน้าที่ในแผนกพัฒนาระบบงาน

6.1.4 ผู้ดูแลด้านเว็บไซต์ ประกอบด้วยเจ้าหน้าที่ในแผนกพัฒนาข้อมูลออนไลน์

6.1.5 ผู้พัฒนาโปรแกรม ประกอบด้วยเจ้าหน้าที่ในแผนกพัฒนาแอปพลิเคชัน

6.2 การควบคุมดูแลการปฏิบัติงานในสำนักสารสนเทศ

6.2.1 เจ้าหน้าที่ดูแลฐานข้อมูล จะต้องไม่เปิดเผยรหัสผ่านเข้าถึงฐานข้อมูลต่อบุคคลอื่น

6.2.2 เจ้าหน้าที่ดูแลฐานข้อมูล มีหน้าที่ดูแลตรวจสอบความผิดปกติของข้อมูล

6.2.3 เจ้าหน้าที่พัฒนาโปรแกรม จะต้องพัฒนาโปรแกรมตามความต้องการที่แสดงเป็นลายลักษณ์อักษร และลงนามรับรองจากผู้จัดการฝ่ายต้นเรื่อง และผู้จัดการสำนักสารสนเทศเท่านั้น

6.2.4 ห้ามเจ้าหน้าที่พัฒนาโปรแกรม ทำการพัฒนาโปรแกรมบนเครื่องแม่ข่ายที่มีฐานข้อมูลจริง โดยจะต้องทำบนเครื่องแม่ข่ายและฐานข้อมูลจำลองเท่านั้น

- 6.2.5 การว่าจ้างพัฒนาระบบจากผู้พัฒนาภายนอก จะต้องมีการกำหนดทีมผู้รับผิดชอบ จากหน่วยงานที่เกี่ยวข้องทั้งหมดร่วมกับสำนักสารสนเทศ เพื่อพิจารณาคัดเลือกผู้พัฒนาและตรวจรับงานร่วมกัน และต้องผ่านการอนุมัติจากกรรมการผู้จัดการเท่านั้น
- 6.2.6 ห้ามมิให้ผู้พัฒนาโปรแกรมภายนอกเข้าถึงระบบและฐานข้อมูลภายหลังส่งมอบเรียบร้อยแล้ว โดยการบริการต่างๆ ของผู้พัฒนาโปรแกรมภายหลังส่งมอบ จะต้องผ่านการอนุมัติจากผู้ดูแลด้านความปลอดภัยเป็นลายลักษณ์อักษรก่อนทุกครั้ง และหากการดำเนินการมีความเสี่ยง และผลกระทบต่อระบบโดยรวม จะต้องได้รับการอนุมัติจากผู้มีอำนาจสูงสุดของสำนักสารสนเทศก่อน และการดำเนินการใดๆ จะต้องอยู่ภายใต้การควบคุมดูแลอย่างใกล้ชิด
- 6.2.7 ผู้ดูแลเว็บไซต์จะต้องทำการตรวจสอบความถูกต้องครบถ้วนของข้อมูลและการลงนามจากผู้มีอำนาจอนุมัติก่อนนำข้อมูลขึ้นเว็บไซต์ทุกครั้ง ห้ามนำข้อมูลที่ยังไม่ได้รับการอนุมัติขึ้นสู่เว็บไซต์

นโยบายฉบับนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ 1 ตุลาคม 2569 เป็นต้นไป



(นางสาวดารณี ฉัตรพิริยะพันธ์)

ประธานเจ้าหน้าที่บริหาร