



<div><div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 1 of 23
<div>1. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)</div> <div>1.1 นโยบายความปลอดภัยสารสนเทศ (Management Directions for Information Security Policy)</div> <div>จุดประสงค์และขอบเขต</div> <p>เพื่ออธิบายถึงจุดประสงค์และขอบเขตของนโยบายความปลอดภัยสารสนเทศในภาพรวม แสดงถึงทิศทางของผู้บริหารขององค์กร ด้านความปลอดภัยสารสนเทศที่ต้องการให้บุคคลที่เกี่ยวข้องกับข้อมูลขององค์กรยึดถือและนำมาใช้ในการปฏิบัติงาน โดยมีเป้าหมายคือ การทำให้การปฏิบัติงานของพนักงานที่เกี่ยวข้องกับข้อมูล รวมถึงระบบที่เกี่ยวข้องกับข้อมูลให้มีความปลอดภัยด้านสารสนเทศที่เพียงพอในการรองรับการดำเนินธุรกิจ ณ ปัจจุบัน และในอนาคตขององค์กร</p> <p>นโยบายความปลอดภัยสารสนเทศ ครอบคลุมถึงการปกป้องข้อมูลขององค์กรเป็นหลัก เนื่องด้วยข้อมูล ถือได้ว่าเป็นทรัพย์สินที่มีความสำคัญเป็นอย่างมากในการดำเนินธุรกิจขององค์กร ซึ่งในกรณีที่มีข้อมูลสำคัญขององค์กร ไม่มีความปลอดภัย ไม่สามารถรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลได้นั้น จะส่งผลกระทบต่อองค์กร ไม่ว่าจะเป็นด้านการเงิน ด้านความเชื่อถือ หรือด้านชื่อเสียงขององค์กร ข้อมูลที่กล่าวถึงในนโยบายนี้ไม่ได้จำกัดอยู่แต่ในรูปแบบอิเล็กทรอนิกส์เท่านั้น ข้อมูลอาจอยู่ในรูปอื่นๆ เช่น เอกสาร สิ่งพิมพ์ ฟิล์ม หรือแม้แต่ในรูปของการสนทนา อย่างไรก็ดี การปกป้องข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ จะกล่าวถึงเป็นส่วนใหญ่ เนื่องจากข้อมูลขององค์กรส่วนใหญ่นั้นจะอยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งในอนาคตจะมีแนวโน้มเพิ่มขึ้นตามลำดับ</p> <p>เนื้อหา นโยบาย และการดำเนินการ</p> <div>1.1.1 การจัดทำนโยบายความปลอดภัยสารสนเทศ (Policies for Information Security)</div> <div>1. นโยบายความปลอดภัยสารสนเทศฉบับนี้ จัดทำเป็นลายลักษณ์อักษรตามจุดประสงค์และขอบเขต และได้รับการอนุมัติจากผู้บริหารหรือคณะกรรมการ มีการประกาศใช้และถือปฏิบัติทั่วทั้งองค์กร โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นขององค์กร ตั้งแต่ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูล และทรัพย์สินสารสนเทศขององค์กร</div> <div>2. ผู้บริหาร พนักงาน ตลอดจนบุคคลภายนอกที่เกี่ยวข้องกับการใช้ข้อมูลและทรัพย์สินสารสนเทศขององค์กร มีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการตามระเบียบว่าด้วยการใช้งานระบบสารสนเทศขององค์กรอย่างปลอดภัย และให้ความร่วมมือในการดำเนินการตามนโยบายอย่างเคร่งครัด การฝ่าฝืนนโยบายนี้ ถือเป็นความผิดที่ร้ายแรง โดยมีบทลงโทษถึงขั้นสูงสุดตามระเบียบขององค์กร</div> <div>1.1.2 การทบทวนนโยบายความปลอดภัยสารสนเทศ (Review of The Policies for Information Security)</div> <p>คณะกรรมการความปลอดภัยสารสนเทศเป็นเจ้าของนโยบายนี้ มีหน้าที่ต้องรับผิดชอบในการดูแลและสอบทวนเนื้อหาของนโยบายอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลง และแนวโน้มของความเสี่ยงในอนาคตที่อาจส่งผลกระทบต่อความปลอดภัยทางด้านสารสนเทศขององค์กร เช่น การเปลี่ยนแปลงกลยุทธ์หรือทิศทางด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กรหรือโครงสร้างเทคโนโลยี เป็นต้น</p>			
Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

 VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin, Prachuap Khiri Khan Thailand 77110		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 2 of 23

2. โครงสร้างความปลอดภัยสารสนเทศ (Organization of Information Security)

2.1 นโยบายโครงสร้างภายในองค์กร (Internal Organization Policy)

จุดประสงค์และขอบเขต

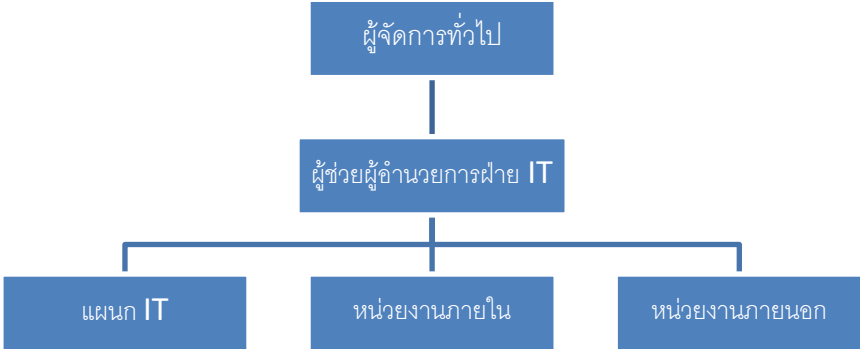
เพื่อให้การจัดการความปลอดภัยสารสนเทศให้เป็นไปอย่างมีระบบและมีความชัดเจน ตั้งแต่ระดับผู้บริหารจนถึงระดับปฏิบัติการองค์กรจึงได้จัดทำโครงสร้างความปลอดภัยสารสนเทศ รวมถึงการกำหนดบทบาท และหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศภายในองค์กร

เนื้อหา นโยบาย และการดำเนินการ

2.1.1 กำหนดบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะกรรมการด้านความปลอดภัยสารสนเทศ ดังนี้

1. ลักษณะโครงสร้างของคณะกรรมการความปลอดภัยสารสนเทศ แสดงดังภาพด้านล่างนี้



```

graph TD
    A[ผู้จัดการทั่วไป] --> B[ผู้ช่วยผู้อำนวยการฝ่าย IT]
    B --> C[แผนก IT]
    B --> D[หน่วยงานภายใน]
    B --> E[หน่วยงานภายนอก]
          
```

2. คณะกรรมการความปลอดภัยสารสนเทศ ประกอบด้วย

2.1 ผู้ช่วยผู้อำนวยการฝ่าย IT


2.2 ผู้ช่วยผู้จัดการพัฒนาโปรแกรม

2.3 เจ้าหน้าที่พัฒนาเว็บไซต์อาวุโส

2.4 เจ้าหน้าที่อาวุโสฝ่ายเทคโนโลยีสารสนเทศ

2.5 เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศ

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/__	(มณฑล รอดสวน) __/__/__	(สุวัฒน์ เจียรนัย) __/__/__	
			Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 3 of 23

3. คณะกรรมการความปลอดภัยสารสนเทศมีหน้าที่ดังนี้

3.1 ตรวจสอบ และอนุมัติ ปรับปรุงนโยบายความปลอดภัยสารสนเทศ ตามกำหนด หรือตามสถานการณ์

3.2 วางแผนประชาสัมพันธ์ และอบรมบุคลากรทุกหน่วยเข้าใจถึงความปลอดภัยสารสนเทศ

3.3 ตรวจสอบ และให้ความเห็นชอบโครงการที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

3.4 วางแผน ตรวจสอบ และบริหารจัดการความเสี่ยงต่างๆ ที่เกิดจากข้อจำกัดของระบบ

3.5 ตรวจสอบ ทบทวน และประเมินแผนความต่อเนื่องด้านความมั่นคงปลอดภัย กรณีฉุกเฉิน

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

คณะกรรมการความปลอดภัย ได้ทำการกำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องตามโครงสร้างของ คณะกรรมการความปลอดภัยสารสนเทศ ดังนี้

1. หน่วยงานด้านเทคโนโลยีสารสนเทศ จัดตั้งขึ้นเพื่อป้องกันความเสียหายขององค์กรอันเกิดจากภัยคุกคามด้านข้อมูล เช่น การสูญหายของข้อมูล หรือการเจาะระบบสารสนเทศ เป็นต้น และทำให้การดำเนินการในส่วนที่เกี่ยวข้องกับข้อมูลมีความปลอดภัยในระดับที่สอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

2. หน่วยงานตรวจสอบ รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายความปลอดภัยสารสนเทศขององค์กร โดย มอบหมายให้ผู้ช่วยผู้อำนวยการฝ่ายบริหาร

3. หน่วยงานภายใน คือพนักงานทุกคนขององค์กร ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง มีหน้าที่รับผิดชอบ ดังนี้

3.1 ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศอย่างเคร่งครัด


3.2 รักษาความลับของข้อมูลสารสนเทศขององค์กร และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง


3.3 รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าวให้กับหน่วยงานด้านเทคโนโลยีสารสนเทศ

3.4 ใช้งานข้อมูล และทรัพย์สินทางข้อมูลขององค์กรอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

4. หน่วยงานภายนอก คือบุคคลภายนอกที่เข้ามาปฏิบัติงานในองค์กรหรือทำงานให้กับองค์กร ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นขององค์กร เช่น ผู้ให้บริการ ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดยมีหน้าที่ความรับผิดชอบเช่นเดียวกับพนักงานขององค์กร

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

<div><div><div><div>VANA NAVA CO.,LTD.</div><div>129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div></div><div><div>Document No.</div><div>SD-ITS-001</div></div></div>		<div>Copied for</div>
<div><div>Document Type:</div><div>มาตรฐาน</div><div>Standard</div></div>		<div><div>Revision No.01</div><div>Effective Date: 15/04/2022</div><div>Page: 4 of 23</div></div>
<div><div>Title:</div><div>นโยบายความมั่นคงปลอดภัยสารสนเทศ</div><div>Information security Policy</div></div>		
<div><div>2.2 นโยบายการจัดชั้นความลับของสารสนเทศ (Information Classification Policy)</div><div><div>จุดประสงค์และขอบเขต</div><div><p>นโยบายได้กำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้น และได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น นอกจากนี้นโยบายยังได้กำหนดถึงบทบาทของเจ้าของข้อมูลและผู้ดูแลข้อมูลที่เกี่ยวข้องกับการจัดลำดับชั้นของข้อมูล เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร</p><p>เนื้อหา นโยบาย และการดำเนินการ</p></div></div><div><div>2.2.1 ชั้นความลับสารสนเทศ (Classification of Information)</div><div><p>สารสนเทศต้องมีการจัดชั้นความลับ โดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต คณะกรรมการได้จัดทำเอกสารแสดง ชั้นความลับสารสนเทศ (DS-ITS-008) เพื่อให้หน่วยงานต่างๆ มาลงทะเบียนเอกสารต่างๆ ตามลำดับชั้นที่กำหนดไว้ ดังนี้</p><div><div>1. ชั้นที่ 1 ข้อมูลเปิดเผยได้</div><div><p>ข้อมูลที่ถูกคนภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่ถูกกฎหมายระบุว่าต้องเปิดเผย</p></div><div><div>2. ชั้นที่ 2 ข้อมูลใช้ภายในองค์กรเท่านั้น</div><div><p>เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้พนักงานทุกคนภายในองค์กรทราบได้ แต่ไม่สามารถเปิดเผยต่อบุคคลภายนอกองค์กรได้ เนื่องจากอาจสร้างความเสียหายให้กับองค์กรได้</p></div><div><div>3. ชั้นที่ 3 ข้อมูลลับ</div><div><p>เป็นข้อมูลใช้ภายในองค์กรที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบ เพื่อให้เพียงพอต่อการปฏิบัติงาน</p></div><div><div>4. ชั้นที่ 4 ข้อมูลลับมาก</div><div><p>เป็นข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้งานบางกลุ่มขององค์กร (ส่วนใหญ่เป็นผู้บริหารเท่านั้น) และไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เนื่องจากข้อมูลประเภทนี้ มีความจำเป็นต่อการปฏิบัติงานขององค์กรและจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียร้ายแรงต่อองค์กร</p></div><div><div>5. ชั้นที่ 5 ข้อมูลลับที่สุด</div><div><p>ข้อมูลใช้ภายในองค์กรแต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้บริหารระดับสูงขององค์กรเท่านั้น และเป็นการใช้เพื่อการวินิจฉัยและตัดสินใจที่สำคัญขององค์กร ไม่สามารถเปิดเผยต่อบุคคลภายนอกได้เลย เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อ</p></div></div></div></div></div></div></div></div></div>		
<div>Written by</div> <div>(กิตติ อินทรสูตร)</div> <div>__/__/__</div>	<div>Reviewed by</div> <div>(มณฑล รอดสวน)</div> <div>__/__/__</div>	<div><div>Approved by</div><div>(สุวัฒน์ เจียรนัย)</div><div>__/__/__</div></div> <div><div>Original Stamp:</div><div>Copy Stamp:</div></div>

<div><div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 5 of 23

การปฏิบัติงานขององค์กรจะเป็นประโยชน์ในเชิงการค้าต่อคู่แข่งหรือทำให้เกิดผลเสียหายนายจ้างต่อองค์กร การนำข้อมูลในชั้นนี้ไปเปิดเผยต่อบุคคลภายนอกไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

3. ความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

3.1 นโยบายก่อนการจ้างงาน (Prior to Employment Policy)

จุดประสงค์และขอบเขต

เพื่อเป็นแนวทางการรักษาความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคลตั้งแต่การรับเข้าทำงานจนถึงการเลิกจ้าง เพราะกระบวนการด้านทรัพยากรบุคคลมีความจำเป็นในการช่วยให้สารสนเทศขององค์กรมีความปลอดภัย

เนื้อหา นโยบาย และการดำเนินการ

3.1.1 การคัดเลือก (Screening)

การตรวจสอบภูมิหลังของผู้สมัครงาน ต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย และระเบียบข้อบังคับ โดยหน่วยงานทรัพยากรบุคคลต้องตรวจสอบประวัติของบุคคลก่อนที่จะทำการว่าจ้าง เช่น หลักฐานการศึกษา บุคคลอ้างอิง ประวัติการทำงานจากหน่วยงานต้นสังกัดเดิม และเอกสารที่ทางราชการออกให้ เป็นต้น โดยเฉพาะตำแหน่งงานที่เกี่ยวข้องกับข้อมูลสำคัญขององค์กร จะต้องมีการตรวจสอบเป็นพิเศษ

3.1.2 ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

ข้อตกลง และเงื่อนไขในสัญญาจ้างกับพนักงาน มีการระบุถึงหน้าที่ความรับผิดชอบ (Job Description) ที่ชัดเจน และระบุถึงความรับผิดชอบด้านความปลอดภัยสารสนเทศ การฝ่าฝืนหรือละเลยต่อหน้าที่และนโยบายถือว่ามีความผิด ต้องพิจารณาตามบทลงโทษขององค์กร ซึ่งขึ้นอยู่กับความรุนแรงของผลกระทบที่เกิดขึ้นกับองค์กร

3.2 นโยบายระหว่างการจ้างงาน (During Employment Policy)

จุดประสงค์และขอบเขต


เพื่อลดความเสี่ยงของสารสนเทศที่เกิดจากบุคลากร ทั้งที่เกิดจากการละเมิดความปลอดภัยสารสนเทศโดยเจตนาและไม่ได้เจตนาหรือจากการละเลยต่อการปฏิบัติหน้าที่ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

เนื้อหา นโยบาย และการดำเนินการ

3.2.1 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

ฝ่ายทรัพยากรบุคคล จัดให้พนักงานทุกคน ต้องเข้ารับฟังการอบรมให้ตระหนักถึงความปลอดภัยสารสนเทศเพิ่ม อย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบถึงนโยบายความปลอดภัยเพิ่มเติมขององค์กรเหตุการณ์ละเมิดความปลอดภัย และกรณีศึกษาใหม่ๆ ในขณะที่หน่วยงานด้านเทคโนโลยีสารสนเทศ จะต้องได้รับการฝึกอบรมจากหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) ____/____/____	(มณฑล รอดสวน) ____/____/____	(สุวัฒน์ เจียรนัย) ____/____/____	
			Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 6 of 23

3.2.3 กระบวนการทางวินัย (Disciplinary Process)

กระบวนการทางวินัยต้องกำหนดอย่างเป็นทางการ พนักงานทุกคนต้องลงลายมือชื่อรับทราบ ระเบียบว่าด้วยการใช้ระบบสารสนเทศขององค์กรอย่างปลอดภัย ซึ่งกระบวนการทางวินัยที่กำหนดขึ้นนี้เพื่อดำเนินการต่อพนักงานที่จะเกิดความมั่นคงปลอดภัยสารสนเทศขององค์กร หน่วยงานทรัพยากรบุคคล และหน่วยงานด้านกฎหมายต้องกำหนดบทลงโทษสำหรับพนักงาน ซึ่งจะเมินนโยบายความมั่นคงปลอดภัยสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 นโยบายหลังการสิ้นสุด หรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment Policy)

จุดประสงค์และขอบเขต

เพื่อเพิ่มความปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการบุคลากรที่กำลังจะเลิกจ้าง โดยระบุหน้าที่ความรับผิดชอบและบทบาทของผู้เกี่ยวข้องกับการระบวนการ นอกจากนี้ยังเป็นการควบคุมความปลอดภัย ของสารสนเทศให้ดียิ่งขึ้น และเพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน


เนื้อหานโยบาย และการดำเนินการ

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

หน่วยงานทรัพยากรบุคคลและหน่วยงานต่างๆ ร่วมกันกำหนดขั้นตอนการปฏิบัติ ของพนักงานที่ออกจากองค์กร เมื่อสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อมีการเปลี่ยนการจ้างงาน ดังนี้

1. หน่วยงานที่เกี่ยวข้อง มีหน้าที่แจ้งไปยังหน่วยงานทรัพยากรบุคคล ถึงเรื่องการลาออก หรือการปรับเปลี่ยนตำแหน่งของพนักงาน
2. หน่วยงานทรัพยากรบุคคล ปฏิบัติตาม นโยบายการบริหารจัดการการเข้าถึงของผู้ใช้ โดยต้องแจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศทราบทันทีที่มีการโอนย้าย ลาออก หรือพ้นสภาพการเป็นพนักงานขององค์กรเพื่อทำการถอดถอนสิทธิ การเข้าใช้ระบบงานต่างๆ และการเข้า ออกพื้นที่องค์กร
3. หน่วยงานด้านเทคโนโลยีสารสนเทศ ปฏิบัติตาม หัวข้อ การคืนทรัพย์สินโดยทำการตรวจสอบทรัพย์สินของพนักงาน และรายงานผลการตรวจสอบกลับมายังหน่วยงานทรัพยากรบุคคล
4. หน่วยงานด้านเทคโนโลยีสารสนเทศ ทำการสำรองข้อมูลที่เป็นของพนักงานดังกล่าว เป็นระยะเวลา 1 ปี และแจ้งให้หน่วยงานที่เกี่ยวข้องทราบถึงวิธีเข้าถึงข้อมูลดังกล่าวได้

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 7 of 23

4. การบริหารจัดการทรัพย์สิน (Asset Management)

4.1 นโยบาย และหน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets Policy)

จุดประสงค์และขอบเขต

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรือแม้แต่อุปกรณ์ที่เกี่ยวข้องในการประมวลผล นอกจากนี้องค์กรควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ตามเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

เนื้อหา นโยบาย และการดำเนินการ

4.1.1 การจัดการบัญชีทรัพย์สิน (Inventory of Assets)

ทุกหน่วยงานขององค์กรที่เกี่ยวข้องกับข้อมูล จะต้องดำเนินการจัดทำบัญชีทรัพย์สิน ที่เกี่ยวข้องกับข้อมูลขององค์กร โดยระบุรายละเอียดต่างๆ ลงทะเบียนทรัพย์สินหน่วยงานเทคโนโลยีสารสนเทศ จะทำการตรวจสอบทรัพย์สิน ร่วมกับผู้ถือครองทรัพย์สิน เพื่อปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of Assets)

ในการจัดทำทะเบียนทรัพย์สิน แต่ละหน่วยงานจะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น เจ้าของทรัพย์สิน ต้องสอบทวนความถูกต้องของรายละเอียดของทรัพย์สินในทะเบียนทรัพย์สินตลอดจนการแจ้งถึงการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับทรัพย์สินให้ผู้ดูแลทรัพย์สินทราบ


4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)


กฎเกณฑ์การใช้ที่เหมาะสมสำหรับการใช้งานสารสนเทศ ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุจัดทำเป็นลายลักษณ์อักษร ผู้ใช้งาน พนักงาน หน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ

4.1.4 การคืนทรัพย์สิน (Return of Assets)

พนักงาน และลูกจ้างของหน่วยงานภายนอก ทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงานหมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง โดยทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะต้องมีการตรวจสอบสภาพทรัพย์สินจากฝ่ายเทคโนโลยีสารสนเทศเสียก่อน หากผลการตรวจสอบพบว่ามี ความชำรุดเสียหาย หรือมีข้อมูลบางอย่างขาดหายไป ผู้รับผิดชอบจะต้องรับผิดชอบตามข้อกำหนดที่ได้ตกลงไว้

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 8 of 23
<div>4.2 นโยบายการจัดการสื่อบันทึกข้อมูล (Media handling Policy)</div> <div>จุดประสงค์และขอบเขต</div> <p>เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล เพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมาจากความเสียหายของสื่อบันทึกข้อมูลต่างๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม</p> <p>เนื้อหา นโยบาย และการดำเนินการ</p> <div>4.2.1 การบริหารจัดการสื่อบันทึกข้อมูล (Management of Media)</div> <p>ขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์การกำหนดไว้</p> <ol style="list-style-type: none">สื่อบันทึกข้อมูลต้องตั้งชื่อตามที่กำหนดและต้องมีทะเบียนควบคุมการใช้งานการเบิกและจ่ายสื่อบันทึกข้อมูลจะต้องผ่านการอนุมัติจากผู้มีอำนาจของหน่วยงานผู้ใช้สื่อบันทึกข้อมูลต้องมีการตรวจนับอย่างน้อยปีละ 1 ครั้ง <div>4.2.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)</div> <p>สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ</p> <ol style="list-style-type: none">ข้อมูลลำดับชั้นลับมากขึ้นไป ที่อยู่ในรูปเอกสารที่ต้องการทำลาย ต้องทำลายโดยการเข้าเครื่องย่อยกระดาษ เมาทำลาย หรือด้วยวิธีการอื่นที่ไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้การทำลายสื่อบันทึกข้อมูลที่บันทึกข้อมูลลำดับชั้นลับมากขึ้นไป ต้องได้รับการอนุมัติจากผู้มีอำนาจและต้องมีการบันทึกการทำลายทุกครั้ง เพื่อเป็นหลักฐานในการตรวจสอบในภายหลัง <div>4.2.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)</div> <p>สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น</p>			
Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 9 of 23

5. การควบคุมการเข้าถึง (Access Control)

5.1 นโยบายความต้องการทางธุรกิจเกี่ยวกับการเข้าถึง (Business Requirements of Access Control Policy)

จุดประสงค์และขอบเขต

เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจประกอบกับข้อกำหนดด้านความปลอดภัย

เนื้อหา นโยบาย และการดำเนินการ

5.1.1 การควบคุมการเข้าถึง (Access Control)

หน่วยงานด้านเทคโนโลยีสารสนเทศจัดทำรายการการเข้าถึงระบบสารสนเทศ ที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ และนำรายการดังกล่าวมาทบทวนตามความต้องการทางธุรกิจ และความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

5.2 นโยบายการควบคุมการเข้าถึงระบบ (System and Application Access Control Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อป้องกันการใช้งานจากผู้ที่ไม่มีความรู้หรือไม่มีสิทธิ์เข้าใช้งานในระดับระบบปฏิบัติการ หน่วยงานด้านเทคโนโลยีสารสนเทศ ควรจัดให้มีการกำหนดข้อความเตือนก่อนการเข้าสู่ระบบ การตรวจสอบผู้ใช้และการบริหารรหัสผ่านสำหรับผู้ใช้งาน รวมถึงการควบคุมเวลาในการเชื่อมต่อสู่ระบบข้อมูล


เนื้อหา นโยบาย และการดำเนินการ

5.2.1 การจัดการการเข้าถึงสารสนเทศ (Information Access Restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ผู้ดูแลระบบ ต้องจัดการให้ระบบแสดงข้อความเตือนถึง “การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิ์เข้าใช้งาน” ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ขององค์กร และระบบต้องเปิดโอกาสให้ผู้ใช้งานสามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่ารระบบนั้นๆ ไม่ได้เกี่ยวข้องกับตนเอง

1. ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้ แต่ละคนได้
2. ผู้ใช้ควรออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก
3. ผู้ใช้ถูกติดตั้งโปรแกรมกั้นหน้าจอ (Screen Server) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์ โดยโปรแกรมเหล่านี้จะเริ่มทำงานหลังจากไม่มีการใช้งานใดๆ บนเครื่องคอมพิวเตอร์นั้นๆ ตามเวลาที่กำหนดไว้
4. หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ หรือเครื่องปลายทางให้เรียบร้อย

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

<div><div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 10 of 23

5.3 นโยบายบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management Policy)

จุดประสงค์และขอบเขต

เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยอาศัยแบบฟอร์ม การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน การควบคุมสิทธิในกระบวนการที่เกี่ยวข้องกับผู้ใช้งานระบบเริ่มตั้งแต่การขอจดทะเบียนไปจนถึงการยกเลิกสิทธิในกรณีที่ผู้ใช้งานนั้นไม่มีความจำเป็นต้องใช้อีกต่อไป รวมไปถึงการควบคุมสิทธิของผู้ใช้ซึ่งมีสิทธิพิเศษที่สามารถแก้ไขสิทธิต่างๆ ของระบบได้

เนื้อหานโยบาย และการดำเนินการ

5.3.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and Deregistration)

กระบวนการลงทะเบียน และถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการใช้สิทธิการเข้าถึง

1. พนักงานทุกคนที่มีสิทธิเข้าใช้งานระบบข้อมูลต้องมีรหัสผู้ใช้เฉพาะบุคคลในการเข้าสู่ระบบ

2. รหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้งานร่วมกัน (Shared User ID) ในกรณีที่พนักงานลาออก รหัสผู้ใช้นั้นต้องไม่ถูกนำกลับมาใช้ใหม่

3. ในการร้องขอเพื่อเข้าใช้งานระบบใดๆ ผู้บังคับบัญชาในหน่วยงานต้องทำการพิจารณาเพื่อเห็นชอบ

4. หน่วยงานเจ้าของข้อมูล และหน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการร่วมกันในการถอดถอนสิทธิของผู้ใช้ ซึ่งไม่มีความต้องการใช้ระบบอีกต่อไปโดยทันที

5.3.2 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง

5.4 นโยบายหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities Policy)

จุดประสงค์และขอบเขต

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต เพื่อมุ่งเน้นให้ผู้ใช้งานระบบมีความตระหนักถึงความปลอดภัยในการใช้งานระบบข้อมูล โดยผู้ใช้ต้องให้ความร่วมมือด้านการใช้รหัสผ่าน และต้องทราบดีถึงวิธีปฏิบัติเมื่อเสร็จภารกิจในการใช้งานคอมพิวเตอร์

เนื้อหานโยบาย และการดำเนินการ

5.4.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of Secret Authentication Information)


ผู้ใช้งานต้องดำเนินการตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูล การพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ ดังต่อไปนี้

1. รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ โดยผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผู้ใช้งานของตน ให้บุคคลอื่น

2. ผู้ใช้ต้องกำหนดและใช้รหัสผ่านที่มีประกอบด้วย ตัวเลข สัญลักษณ์ และตัวอักษร รวมกันมากกว่า 6 ตัวอักษร

3. ผู้ใช้ต้องเปลี่ยนรหัสผ่านของตนเองเป็นประจำ ทุก 90 วัน ไม่ว่าจะมีการบังคับให้เปลี่ยนรหัสผ่านจากระบบหรือไม่ก็ตาม และผู้ใช้ต้องไม่ตั้งรหัสผ่านซ้ำกับของเดิม หรือไม่ใช้วิธีเปลี่ยนตัวเลขต่อท้ายในรหัสผ่าน

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) ____/____/____	(มณฑล รอดสวน) ____/____/____	(สุวัฒน์ เจียรนัย) ____/____/____	
			Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 11 of 23

4. ผู้ใช้ต้องตรวจสอบว่าสิทธิที่ได้รับในการเข้าใช้ระบบเหมาะสมกับหน้าที่ที่ตนรับผิดชอบหรือไม่ ถ้าพบว่าสิทธิที่ได้รับไม่เหมาะสมต้องแจ้งผู้บังคับบัญชาให้ทราบเพื่อพิจารณาและปรับเปลี่ยน ให้เหมาะสม

6. การเข้ารหัสข้อมูล (Cryptography)

6.1 นโยบายมาตรการเข้ารหัส (Cryptographic Controls Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสม และได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศเพื่อรักษาความปลอดภัยของข้อมูลทั้งในด้านความลับและความถูกต้องของข้อมูล จำเป็นต้องพิจารณาถึงการนำซอฟต์แวร์และเทคนิคต่างๆ มาใช้ในการเข้ารหัสข้อมูลที่มีความเสี่ยง

เนื้อหา นโยบาย และการดำเนินการ

6.1.1 การใช้มาตรการเข้ารหัสข้อมูล (Use of Cryptographic Controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

- รหัสผ่านต่างๆ ที่เก็บอยู่ในระบบฐานข้อมูล จะถูกเข้ารหัสไว้ เจ้าของรหัส รวมถึงซอฟต์แวร์เจ้าของข้อมูลเท่านั้นที่ทราบรหัสผ่านดังกล่าว
- เพื่อป้องกันการนำข้อมูลออกสู่ภายนอกจากอุปกรณ์คอมพิวเตอร์ผ่าน USB Port หน่วยงานเทคโนโลยีสารสนเทศ ทำการ Lock ไม่ให้พนักงานสามารถใช้งาน USB Port ได้ (บังคับใช้งานเฉพาะเครื่อง POS เท่านั้น)
- ในการรับส่ง Email ได้ทำการเปิดใช้งานการเข้ารหัส (Encryption) โดยทำการเข้ารหัสในระดับของ Field ข้อมูล


7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)


7.1 นโยบายพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Areas Policy)


จุดประสงค์และขอบเขต


เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร เพื่อกำหนดพื้นที่ควบคุมความมั่นคงปลอดภัยภายในองค์กร และกำหนดมาตรการป้องกันที่เหมาะสมตามระดับความเสี่ยงในแต่ละพื้นที่ โดยการควบคุมดังกล่าวเป็นการป้องกันสารสนเทศ และระบบประมวลผลสารสนเทศขององค์กรชั้นพื้นฐานจากการเข้าถึงโดยไม่ได้รับการอนุญาต ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคาม และการรบกวนไม่ว่าโดยตั้งใจหรือจากภัยธรรมชาติ

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 12 of 23
<p>เนื้อหา นโยบาย และการดำเนินการ</p> <p>7.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)</p> <p>หน่วยงานได้จัดหาที่ตั้งห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากการคุกคามภายนอก คือ อยู่ในสถานที่ที่ เข้าถึงได้โดยยาก จากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้ พื้นที่โดยรอบโปร่ง และสามารถมองเห็นได้ชัดหากมีการเข้าถึงห้อง Server</p> <p>7.1.2 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Office, Room and Facilities)</p> <p>มีการจัดเตรียมอุปกรณ์รักษาความปลอดภัยในการเข้าถึงห้อง Server ดังนี้</p> <ol style="list-style-type: none">มีการติดตั้งกล้องวงจรปิด และบันทึกภาพภายในห้องตลอดเวลา โดยสามารถดูข้อมูลย้อนหลังได้ 30 วันห้องระบบคอมพิวเตอร์ต้องติดตั้งระบบประตูอัตโนมัติ ที่สามารถปิดทันทีโดยอัตโนมัติหลังจากที่เปิดประตูแล้ว และจะต้องมีสัญญาณเตือนเมื่อมีการเปิดประตูทิ้งไว้ <p>7.1.3 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environmental Treats)</p> <p>การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ</p> <ol style="list-style-type: none">ศูนย์คอมพิวเตอร์ ต้องมีระบบป้องกันอัคคีภัย ระบบปรับอากาศและความชื้น ระบบกระแสไฟฟ้าเครื่องปรับอากาศ มี 2 ชุดทำงานสลับกัน โดยตั้งความเย็นอยู่ที่ 20 องศา และมีความชื้นอยู่ที่ 45% <p>7.2 นโยบายเกี่ยวกับการจัดการอุปกรณ์ (Equipment Management Policy)</p> <p>จุดประสงค์และขอบเขต</p> <p>เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อทรัพย์สิน และป้องกันการหยุดชะงักต่อการดำเนินการขององค์กร อุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายถือว่าเป็นอุปกรณ์ที่สำคัญต่อสารสนเทศและการดำเนินธุรกิจ ดังนั้น อุปกรณ์เหล่านี้ควรมีการป้องกันอันตรายจากสภาพแวดล้อม รวมถึงการจำกัดการนำอุปกรณ์ดังกล่าวไปใช้นอกสถานที่</p> <p>เนื้อหา นโยบาย และการดำเนินการ</p> <p>7.2.1 การติดตามการทำงานของเครื่องแม่ข่าย (Server Monitor)</p> <p>มีการจัดทำรายงานสถานการณ์การทำงานของเครื่องแม่ข่ายต่างๆ รวมถึงอุปกรณ์รอบข้างที่จำเป็น เป็นประจำทุกวัน โดยผู้ปฏิบัติจะทำการบันทึกสถานการณ์การทำงานต่างๆ ในรายงานสถานการณ์ทำงานของคอมพิวเตอร์แม่ข่าย (FM-ITS-003) และมีการจัดทำรายงานสรุปสถานการณ์ทำงานของเครื่อง Server ให้กับทางผู้บริหารให้ทราบเป็นประจำทุก 3 เดือน</p> <p>7.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)</p> <p>อุปกรณ์ต้องได้รับการป้องกันการล้มเหลวของกระแสไฟฟ้า และการหยุดชะงักอื่นๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่างๆ</p>			
Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	Copy Stamp:

<div><div><div><div>VANA NAVA CO.,LTD.</div><div>129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div></div><div><div>HUA HIN</div><div>ASIA'S FIRST WATER JUNGLE</div></div></div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 13 of 23
<div><div><div><div><div>1. อุปกรณ์คอมพิวเตอร์และเครือข่ายที่สำคัญต้องมีอุปกรณ์สำรองไฟฟ้าฉุกเฉิน UPS เพื่อให้ระบบทำงานต่อเนื่องหรือสิ้นสุดการทำงานอย่างเหมาะสมเมื่อระบบไฟฟ้าขัดข้อง</div><div>2. ต้องทำการตรวจสอบอุปกรณ์สำรองไฟฟ้าฉุกเฉินตามขั้นตอนของผู้ผลิตอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวสามารถรองรับการทำงานได้เมื่อเกิดปัญหาไฟฟ้าขัดข้อง</div><div>3. ต้องพิจารณาใช้ระบบเครื่องกำเนิดไฟฟ้าสำรอง (Power Generator) กับระบบที่มีความสำคัญในการดำเนินธุรกิจขององค์กรที่มีความจำเป็นต้องทำงานต่อเนื่อง</div><div>4. ต้องทำการทดสอบและตรวจสอบความพร้อมของเครื่องกำเนิดไฟฟ้าสำรอง รวมทั้งแหล่งพลังงานสำรองอย่างน้อยทุกเดือน</div></div></div><div><div>8. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)</div><div><div>8.1 นโยบายการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities Policy)</div><div><div>จุดประสงค์และขอบเขต</div><div><p>เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย เพื่อทำให้เกิดการปฏิบัติงานด้านระบบประมวลผลที่มีความปลอดภัยและถูกต้อง ควรกำหนดหน้าที่ ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบประมวลผลที่ชัดเจน ซึ่งหน้าที่ความรับผิดชอบที่กำหนดนี้ ควรพิจารณาถึงการแบ่งแยกหน้าที่ที่เหมาะสม นอกจากกระบวนการทำงานปกติแล้ว ควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความปลอดภ้ยขึ้นในระบบประมวลผล เพื่อรองรับกับเหตุการณ์ดังกล่าว</p></div><div><div>เนื้อหา นโยบาย และการดำเนินการ</div><div><div>8.1.1 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)</div><div><p>การใช้ทรัพยากรของระบบต้องมีการติดต่อ ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ หน่วยงานเทคโนโลยีสารสนเทศ จึงได้จัดทำ แผนแม่แบบเทคโนโลยีสารสนเทศ (IT Master Plan) เพื่อให้เกิดความมั่นใจว่าสารสนเทศขององค์กรมีความปลอดภัย และสามารถเข้าถึงและใช้งานได้ตามสิทธิโดยง่าย มีการจัดเตรียมซอฟต์แวร์คอมพิวเตอร์ และอุปกรณ์ต่างๆ ที่คอยสนับสนุนการทำงานของหน่วยงานต่างๆ ตามแผนกลยุทธ์ภาพรวมองค์กร</p></div></div></div><div><div>8.2 นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware Policy)</div><div><div>จุดประสงค์และขอบเขต</div><div><p>เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูล จากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตราย</p></div></div></div></div></div></div></div></div>			
Written by		Reviewed by	Approved by
(กิตติ อินทรสูตร) __/__/____		(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____
			Original Stamp:
			Copy Stamp:

<div><div><div><div>VANA NAVA CO.,LTD.</div><div>129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div></div><div><div>HUA HIN</div><div>ASIA'S FIRST WATER JUNGLE</div></div></div> <div><div>Copied for</div><div>Document No. SD-ITS-001</div></div>			
<div>Document Type: มาตรฐาน Standard</div> <div>Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy</div>		<div>Revision No.01</div> <div>Effective Date: 15/04/2022</div> <div>Page: 14 of 23</div>	
<div>เนื้อหา นโยบาย และการดำเนินการ</div> <div>8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware)</div> <div>มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนัก ผู้ใช้งานที่เหมาะสม</div> <div><div>1. หน่วยงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบน เครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา</div><div>2. หน่วยงานเทคโนโลยีสารสนเทศ ต้องกำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบ ประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย</div><div>3. ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตมีการตรวจหา Virus ก่อนนำไปใช้งาน</div><div>4. ห้ามพนักงานดำเนินการใด ที่เกี่ยวกับการพัฒนา Virus หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ</div><div>5. ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง</div></div> <div>8.3 นโยบายการสำรองข้อมูล (Backup Policy)</div> <div>จุดประสงค์และขอบเขต</div> <div>เพื่อป้องกันการสูญหายของข้อมูล เพื่อให้อุปกรณ์ประมวลผลสารสนเทศถูกต้องสมบูรณ์และพร้อมใช้งานเสมอ</div> <div>เนื้อหา นโยบาย และการดำเนินการ</div> <div>8.3.1 การสำรองข้อมูล (Information Backup)</div> <div>ข้อมูลสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้ และมีการทดสอบความพร้อมใช้ของ ข้อมูลอย่างสม่ำเสมอ ตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้</div> <div><div>1. มีการจัดเตรียมแผนในการสำรองข้อมูล และทดสอบกู้คืนระบบ/ข้อมูล แผนสำรองข้อมูลและทดสอบการกู้คืนมีการ ปรับปรุงทบทวนแผนทุกปี</div><div>2. จัดทำคู่มือในการสำรองข้อมูล รวมถึงกู้คืนระบบและข้อมูลกับระบบสำคัญต่างๆ ทั้งหมด โดยจัดทำอยู่ในคู่มือการสำรอง และกู้คืนข้อมูล (MN-ITS-067)</div><div>3. หน่วยงานเทคโนโลยีสารสนเทศ ทำการตรวจสอบการสำรองข้อมูลในระบบทุกวัน ว่ามีสถานะเป็นอย่างไร พร้อมทั้งบันทึก สถานการณ์สำรองข้อมูลลงในรายการสถานการณ์สำรองข้อมูล (FM-ITS-003)</div><div>4. หน่วยงานเทคโนโลยีสารสนเทศ ทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยระบบหลักต้องมีการทดสอบตามแผนการกู้ คืน พร้อมทั้งสรุปเป็นรายงานเพื่อแจ้งคณะกรรมการความมั่นคงสารสนเทศตามกำหนดระยะเวลา</div><div>5. คอมพิวเตอร์ส่วนบุคคล ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญ</div></div>			
<div>Written by</div> <div>(กิตติ อินทรสูตร)</div> <div>__/__/____</div>	<div>Reviewed by</div> <div>(มณฑล รอดสวน)</div> <div>__/__/____</div>	<div>Approved by</div> <div>(สุวัฒน์ เจียรนัย)</div> <div>__/__/____</div>	<div>Original Stamp:</div> <div>Copy Stamp:</div>

 VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin, Prachuap Khiri Khan Thailand 77110		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 15 of 23

8.4 นโยบายการบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

เนื้อหา นโยบาย และการดำเนินการ

8.4.1 การบันทึกข้อมูลล็อก แสดงเหตุการณ์ (Event Logging)

ข้อมูล Log แสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ อุปกรณ์บันทึกข้อมูล Log จะได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไข และการเข้าถึงโดยไม่ได้รับอนุญาต

8.5 นโยบายการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software Policy)

จุดประสงค์และขอบเขต

เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

เนื้อหา นโยบาย และการดำเนินการ

8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

ซอฟต์แวร์คอมพิวเตอร์ทุกเครื่อง จะถูกติดตั้งโดยหน่วยงานเทคโนโลยีสารสนเทศเท่านั้น โดยมีการตรวจสอบตามข้อกำหนดเรื่องการบริหารจัดการทรัพย์สิน (Asset Management)

8.6 นโยบายการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management Policy)

จุดประสงค์และขอบเขต


เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค


เนื้อหา นโยบาย และการดำเนินการ


8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิค จุดอ่อนต่อช่องโหว่ขององค์กร มีการเก็บรวบรวม และการประเมิน และเตรียมมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง โดยช่องโหว่ทั้งหมดจะถูกจัดเก็บไว้ที่เอกสาร ช่องโหว่ทางเทคนิค FM-ITS-013 และช่องโหว่ทั้งหมดจะถูกนำมาทวนสอบกับคณะกรรมการความมั่นคงอย่างน้อยปีละ 1 ครั้ง

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	
			Copy Stamp:

<div><div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 16 of 23
<div>8.7 นโยบายตรวจประเมินระบบสารสนเทศ (Information System Audit considerations Policy)</div> <div>จุดประสงค์และขอบเขต</div> <div>เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินระบบให้บริการ</div> <div>เนื้อหานโยบาย และการดำเนินการ</div> <div>8.7.1 มาตรการตรวจสอบประเมินระบบ (Information System Audit Controls)</div> <div>ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่าง ระมัดระวัง เพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ หน่วยงานเทคโนโลยีสารสนเทศ จะทำการกำหนดแผนการประเมิน ระบบสำคัญต่างๆ ไว้ใน รายการตรวจประเมินระบบและนำผลการตรวจประเมินเสนอคณะกรรมการบริหารความมั่นคงตามกำหนด ระยะเวลา</div> <div>9. ความมั่นคงปลอดภัยสำหรับสารข้อมูล (Communications Security)</div> <div>9.1 นโยบายบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management Policy)</div> <div>จุดประสงค์และขอบเขต</div> <div>เพื่อให้มีการป้องกันสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศ เพื่อให้ระบบเครือข่ายมีความปลอดภัย และสามารถให้ เป็นสื่อในการรับส่งข้อมูลต่างๆ ได้อย่างมีประสิทธิภาพ</div> <div>เนื้อหา นโยบาย และการดำเนินการ</div> <div>9.1.1 มาตรการเครือข่าย (Network Controls)</div> <div>เครือข่ายต้องมีการบริหารจัดการ และควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ หัวหน้าหน่วยงานควบคุมระบบ เครือข่ายต้องรับผิดชอบในการจัดให้มีการควบคุมการปฏิบัติการด้านเครือข่าย ดังต่อไปนี้</div> <div><div>1. กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สาย ที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน โดยจัดทำและปรับปรุง แผนภาพเครือข่ายให้ทันสมัยอยู่เสมอ</div><div>2. จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่จัดไว้</div><div>3. มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสารและอุปกรณ์ใน เครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา</div><div>4. บำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ</div><div>5. ประเมินประสิทธิภาพของระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และวางแผนในการปรับปรุงระบบเครือข่ายให้สามารถ รองรับปริมาณงานที่จะขยายตัวในอนาคต</div></div>			
Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	Copy Stamp:

<div><div><div><div>VANA NAVA CO.,LTD.</div><div>129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div></div><div><div>Document No.</div><div>SD-ITS-001</div></div></div>		<div>Copied for</div>		
<div><div>Document Type:</div><div>มาตรฐาน</div><div>Standard</div></div>		<div><div>Title:</div><div>นโยบายความมั่นคงปลอดภัยสารสนเทศ</div><div>Information security Policy</div></div>		<div><div>Revision No.01</div></div>
		<div><div>Effective Date: 15/04/2022</div></div>		
		<div><div>Page: 17 of 23</div></div>		
<div><div>9.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)</div><div>กลไกด้านความมั่นคงปลอดภัยระดับการให้บริการและความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านั้นจะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม ผู้ให้บริการทางเครือข่าย ต้องได้รับการตรวจสอบ และวิเคราะห์ในเรื่องระดับการให้บริการ รูปแบบความปลอดภัยของเครือข่าย การจัดการความต้องการขององค์กร</div><div>9.2 นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy)</div><div>จุดประสงค์และขอบเขต</div><div>เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กร และถ่ายโอนกับหน่วยงานนอกองค์กร</div><div>เนื้อหา นโยบาย และการดำเนินการ</div><div>9.2.1 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)</div><div>สารสนเทศที่เกี่ยวข้องกับการส่งข้อความอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม</div><div>9.2.2 การตรวจสอบรายการใช้งานเครือข่าย (Network Monitoring)</div><div>หน่วยงานสารสนเทศมีการตรวจสอบการใช้งานเครือข่าย ของฝ่ายต่างๆ และมีการจัดทำ รายงานสรุปการใช้งานเครือข่ายเพื่อนำเสนอต่อคณะกรรมการความมั่นคงตามกำหนดระยะเวลา</div><div>9.3 นโยบายด้านคอมพิวเตอร์พกพาและการปฏิบัติงานจากระยะไกล (Mobile Device and Teleworking Policy)</div><div>จุดประสงค์และขอบเขต</div><div>เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานระยะไกล เช่น Remote เข้ามาทำงานที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) จากทั้งภายใน และภายนอกองค์กร</div><div>เนื้อหา นโยบาย และการดำเนินการ</div><div>9.3.1 การปฏิบัติการจากระยะไกล (Teleworking)</div><div>เป็นมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกล ต้องมีการนำมาใช้เพื่อป้องกันข้อมูลที่มีการเข้าถึงการประมวลผล หรือการจัดเก็บจากสถานที่ดังกล่าว</div><div><div>1. มีการระบุอย่างชัดเจนว่า ใครสามารถที่จะ Remote เข้ามาทำงานได้</div><div>2. กรณีที่ต้องให้หน่วยงานภายนอก Remote เข้ามาต้องมีการบันทึก และมีการเฝ้าดูการทำงานตลอดเวลา และมีการเปลี่ยนแปลง Password ในการเข้าใช้ของหน่วยงานภายนอกทุกครั้ง หรือมีการกำหนด Expired User/Password</div><div>3. มีการกำหนด Session Timeout กรณีที่ผู้ Remote เข้ามาปล่อยหน้าจอทิ้งไว้</div><div>4. จัดทำบันทึกการเชื่อมต่อระยะไกลใน รายการเชื่อมต่อระยะไกล (FM-ITS-005)</div></div></div>				
<div><div>Written by</div><div>(กิตติ อินทรสูตร)</div><div>__/__/____</div></div>		<div><div>Reviewed by</div><div>(มณฑล รอดสวน)</div><div>__/__/____</div></div>	<div><div>Approved by</div><div>(สุวัฒน์ เจียรนัย)</div><div>__/__/____</div></div>	<div><div>Original Stamp:</div></div>
				<div><div>Copy Stamp:</div></div>

 <div> VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110 </div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 18 of 23

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

10.1 นโยบายด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems Policy)

จุดประสงค์และขอบเขต

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการใช้บริการผ่านเครือข่ายสาธารณะด้วย เพื่อให้มั่นใจได้ว่าการพัฒนาระบบงาน ได้คำนึงถึงความปลอดภัย และการควบคุมที่เพียงพอ องค์การต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความปลอดภัยของระบบงาน ก่อนที่จะมีการพัฒนาระบบงาน รวมถึงการกำหนดให้มีการควบคุมภายในของระบบงาน

เนื้อหานโยบาย และการดำเนินการ

10.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่ หรือการปรับปรุงระบบที่มีอยู่แล้ว

- เจ้าของระบบงานธุรกิจ ต้องกำหนดความต้องการด้านความปลอดภัยสารสนเทศ ก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ฟอร์มร้องขอพัฒนาโปรแกรม (FM-ITS-001) ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน
- ความต้องการที่เกิดขึ้น จะต้องได้รับการอนุมัติจากผู้มีสิทธิก่อนส่งมายังหน่วยงานเทคโนโลยีสารสนเทศ เพื่อพิจารณาความเป็นไปได้ในการพัฒนาหรือไม่

10.2 นโยบายสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes Policy)

จุดประสงค์และขอบเขต


เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบ และดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

เนื้อหานโยบาย และการดำเนินการ


10.2.1 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)


การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบ มีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ โดยหน่วยงานเทคโนโลยีสารสนเทศ จะทำการปรับปรุงเอกสาร การควบคุมเวอร์ชันของระบบ (FM-ITS-009)

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) _/_/_	(มณฑล รอดสวน) _/_/_	(สุวัฒน์ เจียรนัย) _/_/_	Copy Stamp:

<div><div><div><div>VANA NAVA CO.,LTD.</div><div>129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div></div></div><div><div>Document No.</div><div>SD-ITS-001</div></div></div>		<div>Copied for</div>	
<div><div>Document Type:</div><div>มาตรฐาน</div><div>Standard</div></div>		<div><div>Title:</div><div>นโยบายความมั่นคงปลอดภัยสารสนเทศ</div><div>Information security Policy</div></div>	<div><div>Revision No.01</div><div>Effective Date: 15/04/2022</div><div>Page: 19 of 23</div></div>
<div>10.2.2 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)</div> <div>แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชันใหม่</div> <div><div>1. กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อให้มั่นใจว่า ข้อมูลมีความถูกต้องสมบูรณ์ ทั้งนี้ การตรวจสอบควรครอบคลุมถึง</div><div>2. ผู้ร้องขอ จะต้องเป็นผู้ทดสอบ และตรวจรับระบบในฟอร์มร้องขอพัฒนาโปรแกรม (FM-ITS-009)</div></div> <div>10.3 นโยบายสำหรับการทดสอบข้อมูล (Test Data Policy)</div> <div><div>จุดประสงค์และขอบเขต</div><div>เพื่อให้มีการป้องกันข้อมูลที่น่ามาใช้ในการทดสอบ</div><div>เนื้อหา นโยบาย และการดำเนินการ</div><div>10.3.1 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)</div><div>สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต</div><div><div>1. ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)</div><div>2. ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการถอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง</div><div>3. ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่นๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง</div></div></div> <div>11. ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)</div> <div><div>11.1 นโยบายเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship Policy)</div><div><div>จุดประสงค์และขอบเขต</div><div>เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก</div><div>เนื้อหา นโยบาย และการดำเนินการ</div><div>11.1.1 ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)</div><div>ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายใน และจัดทำเป็นลายลักษณ์อักษร</div></div></div>			
<div>Written by</div> <div>(กิตติ อินทรสูตร)</div> <div>__/__/____</div>	<div>Reviewed by</div> <div>(มณฑล รอดสวน)</div> <div>__/__/____</div>	<div>Approved by</div> <div>(สุวัฒน์ เจียรนัย)</div> <div>__/__/____</div>	<div>Original Stamp:</div> <div>Copy Stamp:</div>

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทสรุตร) / /	(มณฑล รอดสวน) / /	(สุวัฒน์ เจริญชัย) / /	Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 21 of 23
<p>สรุปดังกล่าว เพื่อนำเสนอคณะกรรมการความมั่นคงปลอดภัยสารสนเทศ เป็นประจำทุก 3 เดือน เพื่อร่วมพิจารณาปัญหาและวาง แนวทางป้องกันปัญหาที่เกิดขึ้นในอนาคต</p> <p>13. การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)</p> <p>13.1 นโยบายความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity Policy)</p> <p>จุดประสงค์และขอบเขต</p> <p>เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ไม่ว่าจะเป็นด้วย อุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหาย ต่อองค์กรไม่มากนักน้อย ดังนั้น จึงควรจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับ ที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักขององค์กรต่อไปได้</p> <p>เนื้อหานโยบาย และการดำเนินการ</p> <p>13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)</p> <p>องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสภาพการณ์ความเสียหายที่ เกิดขึ้น เช่น ในช่วงที่เกิดภัยพิบัติ ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่างๆ เพื่อพัฒนาและคงไว้ซึ่งความ ต่อเนื่องทางธุรกิจ การจัดการกระบวนการต่างๆ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจดังกล่าว ต้องคำนึงถึงสิ่งต่างๆ ดังต่อไปนี้</p> <ol style="list-style-type: none">1. การวิเคราะห์และการประเมินความเสี่ยงที่กระทบต่อการดำเนินธุรกิจขององค์กร2. การจัดทำเอกสารกลยุทธ์เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ ต้องสอดคล้องกับเป้าหมายทางธุรกิจ ขององค์กร3. การฝึกอบรมพนักงาน เพื่อให้ตระหนักถึงความมั่นคงปลอดภัย และเข้าใจในแผนฯ พร้อมทั้งสามารถปฏิบัติตามแผนฯ ได้4. การกำหนดหน้าที่ความรับผิดชอบในการประสานงาน การพัฒนา การตรวจทาน และการปรับปรุงแผน <p>13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)</p> <p>องค์กรต้องกำหนด จัดทำการบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (DS-ITS-006) และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมี สถานการณ์ความเสียหายหนึ่งเกิดขึ้น</p> <ol style="list-style-type: none">1. มีการสื่อสารไปยังพนักงานทุกคนทราบถึงแผนการดำเนินการเมื่อเกิดเหตุฉุกเฉิน2. แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่างๆ ต้องมีการทดลอง ชักซ้อม ตามระยะเวลาที่กำหนด3. เจ้าของแผนงานและแนวทางปฏิบัติซึ่งเจ้าของแผนฯ ต้องรับผิดชอบในการบำรุงรักษา และทดสอบพัฒนาหลักเกณฑ์ ความต้องการและเงื่อนไขสำหรับการนำแผนฯ ไปใช้			
Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	Copy Stamp:

 VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin, Prachuap Khiri Khan Thailand 77110		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 22 of 23

13.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมไว้ (DS-ITS-006) ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้อง และได้รับผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น พื้นฐานของการจัดการเพื่อให้เกิดความต่อเนื่องในการดำเนินธุรกิจคือ เข้าใจถึงกระบวนการ และเหตุการณ์ที่สามารถก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ ดังนั้นหน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้นต้องเข้าร่วมในการดำเนินการระบุเหตุการณ์ที่อาจส่งผลกระทบต่อกระบวนการทางธุรกิจ ตลอดจนการประเมินความเสี่ยงเพื่อให้ได้มา ซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องทางธุรกิจในการดำเนินธุรกิจลำดับต่อไป

13.2 นโยบายการเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies Policy)

จุดประสงค์และขอบเขต

เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

เนื่อหานโยบาย และการดำเนินการ

13.2.1 สภาพพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

14. ความสอดคล้อง (Compliance)

14.1 นโยบายความสอดคล้องด้านกฎหมายและสัญญาจ้าง (Compliance with Legal and Contractual Requirements Policy)

จุดประสงค์และขอบเขต


เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและที่เป็นความต้องการด้านความมั่นคงปลอดภัย

เนื่อหานโยบาย และการดำเนินการ

14.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of Applicable Legislation and Contractual Requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง รวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบและสำหรับ

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/____	(มณฑล รอดสวน) __/__/____	(สุวัฒน์ เจียรนัย) __/__/____	
			Copy Stamp:

 <div>VANA NAVA CO.,LTD. 129/99 Soi Moo Baan Nong Kae, Nong Kae, Hua Hin,Prachuap Khiri Khan Thailand 77110</div>		Copied for	Document No. SD-ITS-001
			Revision No.01
Document Type: มาตรฐาน Standard	Title: นโยบายความมั่นคงปลอดภัยสารสนเทศ Information security Policy		Effective Date: 15/04/2022
			Page: 23 of 23

หน่วยงาน องค์การกำหนดให้เอกสารสัญญาต่างๆ ที่มีผลเกี่ยวข้องกับกฎหมาย ลิขสิทธิ์ซอฟต์แวร์ และสิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights) ถูกจัดเก็บไว้ที่ หน่วยงานเทคโนโลยีสารสนเทศโดยจะจัดเก็บอยู่ในแบบฟอร์มรายการสัญญา

14.2 นโยบายการทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews Policy)

จุดประสงค์และขอบเขต

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบาย และขั้นตอนปฏิบัติขององค์กร

เนื้อหา นโยบาย และการดำเนินการ

14.2.1 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)

ผู้จัดการฝ่ายต่างๆ มีหน้าที่ต้องดำเนินการทบทวนความสอดคล้องของขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง คณะกรรมการความมั่นคงปลอดภัยกำหนดให้ หน่วยงานความปลอดภัยสารสนเทศ นำเสนอระบบโครงสร้างสารสนเทศ ระบบความปลอดภัยหลัก เทคโนโลยีใหม่ๆ รวมถึงข้อมูลเชิงเทคนิค กับคณะกรรมการความมั่นคงปลอดภัย ปีละ 1 ครั้ง เพื่อใช้เป็นข้อมูลในการพิจารณาความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยคณะกรรมการความปลอดภัยสารสนเทศ ได้จัดทำรายการต่างๆ ที่จะต้องปฏิบัติไว้ในแบบฟอร์ม การทวนสอบความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้เป็นตัวกลางในการตรวจสอบการทวนสอบขั้นตอนต่างๆ ว่าได้ปฏิบัติตามครบถ้วนหรือไม่

Written by	Reviewed by	Approved by	Original Stamp:
(กิตติ อินทรสูตร) __/__/__	(มณฑล รอดสวน) __/__/__	(สุวัฒน์ เจียรนัย) __/__/__	Copy Stamp: