บริษัท วี.แอล. เอ็นเตอร์ไพรส์ จำกัด (มหาชน)

V.L. ENTERPRISE PUBLIC COMPANY LIMITED

# นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

## VL-IT-PO-01

| จัดทำโดย | สอบทานโดย | อนุมัติโดย |
|---|---|---|
| (กัณธี วิจิตสกุลชัย) | (.....) | (.....) |
| นายกัณธี วิจิตสกุลชัย | นางสาวรักชนก สำเนียงล้ำ | นางชุติภา กลิ่นสุวรรณ |
| วันที่ | วันที่ | วันที่ |
| 16 มกราคม 2563 | 16 มกราคม 2563 | 16 มกราคม 2563 |

# นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

## สารบัญ

## บทนำ

1. นโยบายนี้จัดทำขึ้นสำหรับพนักงานหรือบุคคลอื่นที่บริษัทฯอนุญาตให้เข้าใช้งานระบบเครือข่ายและ คอมพิวเตอร์ และระบบข้อมูลของบริษัทฯรวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตโดยผ่านทาง เครือข่ายของบริษัทฯโดยให้ถือปฏิบัติอย่างเคร่งครัด
2. บริษัทฯดำเนินกิจการภายใต้กฎหมายไทยดังนั้นการใช้งานระบบเครือข่ายและคอมพิวเตอร์ รวมทั้งการ เชื่อมต่อทางอินเทอร์เน็ตจึงให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผล บังคับใช้ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง
3. ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อเป็นทรัพย์สินของบริษัทฯจัดหาไว้เพื่อ บริการที่เกี่ยวข้องกับกิจการของบริษัทฯเท่านั้น
4. บริษัทฯสงวนสิทธิในการเข้าตรวจสอบ เก็บหลักฐาน และดำเนินการอันสมควร หากพบว่ามีการละเมิด นโยบายการใช้งานระบบเครือข่ายและคอมพิวเตอร์ และการเชื่อมต่ออินเทอร์เน็ต

## คำอธิบาย

1. "บริษัทฯ" หมายถึง บริษัท วี.แอล. เอ็นเตอร์ไพรส์ จำกัด รวมถึง บริษัทย่อย และบริษัทในเครือ ที่ใช้ระบบ เครือข่ายคอมพิวเตอร์และระบบข้อมูลร่วมกัน
2. "ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัทฯ
3. "พนักงาน" หมายถึง พนักงาน ลูกจ้างทดลองงาน และลูกจ้างชั่วคราวของบริษัทฯ
4. "ระบบเครือข่ายและคอมพิวเตอร์" หมายถึง เครื่องคอมพิวเตอร์ที่เป็นสมบัติของบริษัทฯ รวมทั้งอุปกรณ์ ต่อพ่วงต่างๆ ตลอดจนอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่างๆ ภายในบริษัทฯ รวมทั้งการ เชื่อมโยงคอมพิวเตอร์ในระยะไกลเข้าด้วยกัน
5. "ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงข้อมูลหรือสิ่งใดๆ ไม่ว่าการสื่อความหมาย นั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของ เอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
6. "ระบบข้อมูล" หมายถึง ระบบงานโปรแกรมคอมพิวเตอร์ของบริษัทฯที่ทำงานเกี่ยวข้องกับ การเก็บ (นำเข้า)จัดการ (ประมวลผล) และเผยแพร่ (แสดงผล) ข้อมูลและสารสนเทศ เพื่อสนับสนุนกลไกการ ทำงานของบริษัท
7. "ผู้ดูแลระบบ" หมายถึง ผู้จัดการส่วนระบบเครือข่ายและคอมพิวเตอร์ ผู้จัดการส่วนจัดการระบบข้อมูล หรือพนักงานอื่นที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป ให้มีหน้าที่รับผิดชอบ ในการดูแลรักษาคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย คอมพิวเตอร์เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ และ/หรือได้รับมอบหมายให้มีหน้าที่ รับผิดชอบในการพัฒนาแก้ไขและดูแลระบบข้อมูลและโปรแกรมต่างๆที่ใช้งานอยู่ในบริษัทฯ หรือ หน่วยงานที่มีหน้าที่และรับผิดชอบในการดูแลคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์หรือระบบข้อมูลโดยตรง

## วัตถุประสงค์

บริษัทฯ ได้จัดให้มีระบบเครือข่ายและคอมพิวเตอร์เพื่อสนับสนุนประสิทธิภาพการดำเนินงานของบริษัทฯ ให้สามารถตอบสนองฟ้าหมายทางธุรกิจได้ดีที่สุด จังนั้น บริษัทฯ จึงถือว่าระบบเครือข่ายและคอมพิวเตอร์เป็นทรัพย์สินที่สำคัญของบริษัทฯ ซึ่งผู้ปฏิบัติงานจะต้องใช้และดูแลรักษาให้อยู่ในสภาพที่พร้อมใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา ด้วยเหตุนี้จึงได้จัดทำนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยสารสนเทศโดยมีวตถุประสงค์สำคัญจังนี้

1. เพื่อให้มีนโยบายและแนวปฏิบัติในก"รรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกียวข้อง
2. เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและบุคคลที่ปฏิบัติงานให้คับบริษัท รวมมั้งการยืนยันคัวบุคคลากรเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแพนเตรียมความพร้อมกรณีฉุกเฉินใน กรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบกลับคืนมาได้ภายใน ระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องคับการใช้งานตามภารกิจของบริษัท
4. เพื่อให้มีการตรวจสอบและประเมินความเสียงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบ เทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
5. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการ รักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกียวข้อง

นโยบายนี้ครอบคลุมการควบคุมการเข้าถึงระบบและทรัพยากรสารสนเทศที่เป็นโปรแกรมประยุกต์ (Application) เครือข่ายคอมพิวเตอร์ (Computer Network) และเครือข่ายไร้สาย (Wireless Network) เครื่อง คอมพิวเตอร์ เครื่อง คอมพิวเตอร์แม่ข่าย ที่เป็นของบริษัทเพื่อความมั่นคงปลอดภัยของข้อมูลและเครือข่าย ของบรีษัท

## นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและศูนย์คอมพิวเตอร์

1. พื้นที่ในการวาง Server ควรตั้งอยู่ในสถานที่ที่เหมาะสม ไม่มีฝุ่นควัน และมีเครื่องปรับอากาศทำงาน
2. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ
3. มีกุญแจปิดล็อก หรือมีระบบคีย์การ์ด กำหนดสิทธิ์ การเข้าออกได้ เพื่อง่ายและสะดวกต่อการเฝ้าระวัง ควบคุม รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้
4. การรักษาความปลอดภัยการเข้าออกจากผู้อื่น ด้วยการบันทึกวัตถุประสงค์ในการเข้าออกทุกครั้ง
5. มีระบบป้องกันอัคคีภัย และถังดับเพลิงในกรณีเกิดเหตุฉุกเฉิน
6. มีเครื่องสำรองไฟในกรณีฉุกเฉินให้กับ Server และ PC รวมถึงอุปกรณ์ต่าง ๆ ที่เชื่อมต่อลงกับระบบ เครือข่าย

## นโยบายการควบคุมการใช้งานระบบเครือข่ายและคอมพิวเตอร์

1. การใช้งานระบบเครือข่ายจะต้องใช้งานผ่านเครื่องคอมพิวเตอร์ของบริษัทฯ เท่านั้น การใช้งานระบบ เครือข่ายจากเครื่องคอมพิวเตอร์ที่ไม่ใช่เครื่องคอมพิวเตอร์ของบริษัทฯ จะต้องได้รับอนุญาตจากผู้ดูแล ระบบก่อน
2. กำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศของบริษัทสำหรับผู้ใช้บริการ โดยต้องได้รับอนุญาต ให้เข้าถึงระบบด้วยวิธีการดังต่อไปนี้
   - สำหรับบุคลากรให้ ขออนุญาตการเข้าถึงระบบตามระเบียบการขอใช้ บริการของฝ่ายระบบ เทคโนโลยีสารสนเทศ
   - สำหรับผู้ใช้บริการชั่วคราว ให้ขออนุญาตการเข้าถึงระบบตามระเบียบการขอใช้บริการของฝ่าย ระบบเทคโนโลยีสารสนเทศ
3. ต้องกำหนดให้มีผู้ดูแลระบบในกรณีที่หน่วยงานจัดตั้งเครือข่ายของหน่วยงานที่เชื่อมต่อกับเครือข่ายหลัก โดยให้ผู้ดูแลระบบปฏิบัติตามข้อดังต่อไปนี้
   - ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น โปรแกรมประยุกต์ (Application) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดย ต้องให้สิทธิเฉพาะสิทธิ์เท่าที่จำเป็นตามกรอบนโยบายฉบับนี้รวมทั้งผู้ดูแลระบบต้องทบทวนสิทธิ์ ดังกล่าวอย่างสม่ำเสมอ

- ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบ สารสนเทศ รวมทั้งผู้ดูแลระบบต้องมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
- การเพิ่ม/ลดสิทธิการใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรเท่านั้น และ ส่งต่อให้ผู้ดูแลระบบรับทราบและดำเนินการเพิ่มสิทธิ์
- ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ
- ผู้ดูแลระบบต้องให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความ จำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยน ตำแหน่งงานภายในหน่วยงาน เป็นต้น

4. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้น ระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้ บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
5. ผู้ดูแลระบบ ต้องควบคุมการเชื่อมต่อเครือข่ายกับระบบเครือข่ายหลัก เพื่อบริหารจัดการระบบเครือข่าย ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้
   - ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
   - ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่อง คอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้
   - ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก ( Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ
   - การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของ ผู้ใช้บริการ
   - เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานต้องมีการป้องกันมิให้ หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบ เครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย
- การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบและ จำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. ห้ามใช้ทรัพยากรสารสนเทศและระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของ ประเทศ กฎหมาย หรือกระทบต่อภารกิจของบริษัท
7. ห้ามใช้ทรัพยากรสารสนเทศและระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและ ศีลธรรม หรือกระทบต่อภารกิจของบริษัท
8. ห้ามใช้ทรัพยากรสารสนเทศทุกประเภทที่เป็นของบริษัทเพื่อประโยชน์ทางการค้า
9. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม
10. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทต้องหยุดชะงัก
11. ห้ามใช้ระบบสารสนเทศของบริษัทเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้ รับอนุญาตจากผู้มีอำนาจ
12. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็น กรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม
13. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทโดยไม่ได้รับ อนุญาต
14. ไม่นำอุปกรณ์เชื่อมต่อข้อมูล จำพวก Flash Drive หรือ External Drive จากภายนอกมาใช้งานโอนถ่าย ข้อมูลกับ Server โดยไม่จำเป็น รวมถึงเครื่อง PC

นโยบายการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

1. ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล
2. บริษัทต้องกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจร ทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้
   - ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้ เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
   - ควรจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้น ความลับในการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย
   - ควรกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการ พยายามเข้าสู่ระบบ บันทึกการใช้งาน Commard Line และ Firewall Log เป็นต้น เพื่อประโยชน์ใน การใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง
   - ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ
3. ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัด เส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักที่ มีผลให้การทำงานของเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

## นโยบายด้านการพิสูจน์ตัวตน (AUTHENTICATION, IDENTIFICATION AND ACCOUNTABILITY)

1. นโยบายนี้กำหนดให้การพิสูจน์ตัวตน (Authentication) ต้องกระทำในกรณีต่างๆ ดังต่อไปนี้
   - คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
   - การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้ง

- การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้บริการได้ และบ่งบอกถึงเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ และอาจบ่งบอกถึง ตำแหน่งที่ตั้งของเครื่องคอมพิวเตอร์

2. ต้องมีการกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือ พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
3. ต้องกำหนดรหัสผู้ใช้งาน (User Account) ต้องไม่ซ้ำกัน
4. ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ ป้องกันการเข้าถึง และไม่เขียนหรือพิมพ์รหัสผ่านแสดงไว้ให้บุคคลอื่นเห็น
5. มีการตั้งรหัสผ่านการใช้งานเครือข่ายและการใช้งานโปรแกรม โดยพาสเวิร์ดต้องประกอบด้วย ตัวอักษร และตัวเลข ความยาวไม่ต่ำกว่า 6 ตัวอักษร
6. ผู้ใช้บริการต้องเปลี่ยนรหัสผ่าน (Password) อย่างน้อยทุกๆ 6 เดือนหรือทุกครั้งที่มีการแจ้งเตือนให้ เปลี่ยนรหัสผ่าน
7. เมื่อผู้ใช้บริการไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการปิดกั้นจอภาพ (Screen Lock) ทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง โดยเครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักจอภาพ (Screen Saver) โดยตั้งเวลาอย่างน้อย 5-10 นาที
8. ผู้ใช้บริการต้องมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้ ( Username) และรหัสผ่าน (Password) โดยผู้ใช้บริการแต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่หรือแจกจ่ายเป็นเหตุให้ผู้อื่นล่วงรู้รหัสผ่าน
9. ผู้ใช้บริการต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้บริการหรือไม่ก็ตาม
10. ผู้ใช้บริการต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพยากรหรือระบบสารสนเทศของบริษัท และ หากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากการลืมรหัสผ่าน หรือชื่อบัญชีโดนล็อค หรือเกิดจาก ความผิดพลาดใดๆ ผู้ใช้บริการต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ 9 สำหรับผู้ใช้บริการภายนอกเบบชั่วคราวให้กำหนดให้มีผู้รับผิดชอบชื่อบัญชีชั่วคราว (Temporary Account)แทนได้ เช่นกรณีการจัดสัมมนาหรืออบรม โดยให้หัวหน้าโครงการจัดสัมมนาหรืออบรมเป็น

ผู้รับผิดชอบการพิสูจน์ตัวตนของผู้เข้าสัมมนาหรืออบรม และหากมีการกระทำผิดอันใดของผู้ใช้งาน ภายนอก ให้ผู้รับผิดชอบแทนเป็นผู้รับผิดต่อการกระทำดังกล่าว

## นโยบายการสำรองข้อมูลและกู้คืนข้อมูล

1. ผู้ดูแลระบบต้องมีการ Backup ข้อมูล Server อย่างสม่ำเสมอ (ตามแผนการสำรองข้อมูลและการกู้คืน ระบบ)
2. ผู้ดูแลระบบต้องทำสำเนาซอฟต์แวร์ของระบบสารสนเทศของบริษัทหรือของหน่วยงานที่มีความสำคัญ อย่างสม่ำเสมอหรือก่อนการเปลี่ยนแปลงหรือปรับปรุงเวอร์ชั่นของซอฟต์แวร์เพื่อป้องกันปัญหาระบบไม่ สามารถใช้งานได้หรือไม่สามารถกู้คืนได้เมื่อเกิดปัญหาเมื่อทำการปรับปรุง
3. ผู้ดูแลระบบต้องทำการสำรองข้อมูลต่างๆ ที่สำคัญของระบบสารสนเทศอย่างสม่ำเสมอ สำหรับข้อมูลที่ มีอัตราการเปลี่ยนแปลงมากให้สำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง
4. ผู้ดูแลระบบต้องมีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบ ซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยกำหนดให้มีขั้นตอนการปฏิบัติแยกตามระบบสารสนเทศ แต่ละระบบ
5. ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่นที่ไม่ใช่สถานที่เดียวกับสถานที่ติดตั้งระบบหรืออยู่ในสถานที่ที่ปลอดภัยจากภาวะคุมคาม (Threat) ต่างๆ ที่อาจเกิดขึ้นกับระบบหรือ สถานที่ติดตั้งระบบได้
6. ต้องมีการจัดทำแผนและระบบการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอเพื่อพิสูจน์ว่าสื่อที่เก็บ สำรองข้อมูลยังสามารถใช้งานได้
7. บริษัทและหน่วยงานต้องมีการจัดทำแผนการกู้คืนระบบกรณีเกิดเหตุหายนะ (Disaster Recovery Plan) ให้สามารถกู้ระบบกลับคืนมาภายในระยะเวลาที่เหมาะสม