บริษัท บางกอก เฮลท์ กรุ๊ป จำกัด

Bangkok Health Group Co., Ltd

นโยบายความมั่นคงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. นโยบายความมั่นคงและความปลอดภัยด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทเป็นการจัดทำเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ให้อยู่ในระดับมาตรฐานสากล อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็ว หลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศของบริษัท นโยบายความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทฯ โดยมีรายละเอียดดังต่อไปนี้

หมวดที่ 1 ว่าด้วยการพิสูจน์ตัวตน (Accountability, Identification and Authentication)

ข้อ 1. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ 2. ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ 3. ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษร ไม่น้อยกว่า 7 ตัวอักษรสำหรับเจ้าหน้าที่บริษัทที่ได้รับสิทธิ์ปกติ (Regular Users) และ (Privileged Users) ซึ่งรหัสต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character) ทั้งตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ซึ่งรหัสผ่านไม่ควรมีตัวอักษรที่ซ้ำๆ กัน เช่น “AAA BBB” และเรียงตามลำดับอักษรหรือตัวเลข เช่น “ABCDE”,”12345” เป็นต้น

ข้อ 4. ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว (Recycle Password) ต้องไม่ซ้ำกับบัญชีรายชื่อผู้ใช้ระบบงาน (User ID) และต้องไม่กำหนดรหัสผ่านเป็นค่าว่าง (Blank Password)

ข้อ 5. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ 6. ผู้ใช้งานต้องการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สิน หรือระบบสารสนเทศของบริษัทฯ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

1) เมื่อได้รับรหัสผ่าน ต้องกำหนดให้มีการเปลี่ยนรหัสผ่านเมื่อมีการใช้งานเป็นครั้งแรก
2) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
3) การใช้งานระบบคอมพิวเตอร์อื่น ในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
4) เมื่อผู้ใช้งาน ไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการล็อคหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
5) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen saver) โดยตั้งเวลาอย่างน้อย 5 นาที
6) หากมีไฟล์ที่เก็บรหัสผ่านต้องทำการตั้งรหัสก่อนเปิดทุกครั้ง

หมวดที่ 2 ว่าด้วยการบริหารจัดการทรัพย์สิน (Assets Management)

ข้อ 7. ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของบริษัทฯ ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 8. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใด ออกจากห้องคอมพิวเตอร์แม่ข่าย (sever) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 9. ผู้ใช้งานไม่ต้องนำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

ข้อ10. ผู้ใช้งานไม่ต้องใช้ หรือลบแฟ้มข้อมูลไม่ว่ากรณีใดๆ

ข้อ11. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต

ข้อ12. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่บริษัทฯ มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยบรรดารายการทรัพย์สิน (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนทรัพย์สินถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่บริษัทฯ ที่ได้รับมอบหมาย

ข้อ13. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของบริษัทฯ ที่ได้รับมอบหมาย

ข้อ14. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ 15. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน้ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ 16. ทรัพย์สินและระบบสารสนเทศต่างๆที่บริษัทฯ จัดเตรียมไว้ให้ใช้งาน มีวัตถุประสงค์เพื่อการใช้งานของบริษัทฯ เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่บริษัทฯ ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อบริษัทฯ

ข้อ 17. ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ 16 ให้ถือว่าเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวดที่ 3 ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ 18. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของบริษัทฯ หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ 19. ข้อมูลทั้งหลายที่อยู่ภายในสินทรัพย์ของบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 20. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของบริษัทฯ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ 21. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ 22. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร บริษัทฯจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลใดบุคคลหนึ่งกระทำการละเมิดต่อข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่บริษัทฯ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับบริษัทฯ ซึ่งบริษัทฯ อาจแต่งตั้งผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวดที่ 4 ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ 23. ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการ ดังนี้

1.) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัย รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือ แกะรหัสผ่านของบุคคลอื่น

2.) พัฒนาโปรแกรม หรือ ฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

3.) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะ เช่น เดียวกับหนอน หรือไวรัสคอมพิวเตอร์

4.) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

5.) เสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือ ขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ 24. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit torrent) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 25. ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างทำงาน

ข้อ 26. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์ รวมถึงอุปกรณ์อื่นใดของ บริษัทฯ ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมายหรือกระทบต่อภารกิจของบริษัทฯ

ข้อ 27. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของบริษัทฯ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรมหรือกระทบต่อภารกิจของบริษัทฯ

ข้อ 28. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทฯ เพื่อประโยชน์ทางการค้า

ข้อ 29. ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

ข้อ 30. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของบริษัทฯ ต้องหยุดชะงัก

ข้อ 31. ห้ามใช้ระบบสารสนเทศของบริษัทฯ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่รับอนุญาตจากผู้มีอำนาจ

ข้อ 32. ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ 33. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวดที่ 5 ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ 34. บรรดากฎหมายและข้อบังคับใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของบริษัทฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวดที่ 6 ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing Intellectual Property)

ข้อ 35. บริษัทฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่บริษัทฯ อนุญาตให้ใช้งาน หรือที่บริษัทฯ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และบริษัทฯ ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ บริษัทฯ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ 36. ซอฟต์แวร์ (Software) ที่บริษัทฯ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้งถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

หมวดที่ 7 ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

ข้อ 37. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus) ตามที่บริษัทฯ ได้ประกาศให้ใช้ โดยจะทำการ Scan virus สัปดาห์ละ 1 ครั้ง เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 38. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ 39. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ 40. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ 41. เมื่อผู้ใช้งานพบว่า เครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ 42. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของบริษัท หรือของผู้อื่นโดยไม่รับอนุญาตจากผู้มีอำนาจ

ข้อ 43. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของบริษัทฯ

2. นโยบายความมั่นคงปลอดภัยของเครือขายไร้สาย (Wireless Policy)

ข้อ 1. ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของงอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายให้น้อยที่สุด

ข้อ 2. ผู้ดูแลระบบ (System Administrator) ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ 3. ผู้ดูแลแลระบบ (System Administrator) ต้องตั้งค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ 4. ผู้ดูแลระบบ (System Administrator) ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ 5. ผู้ดูแลระบบ (System Administrator) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้บัญชาการทราบทันที

ข้อ 6. ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

3. นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ข้อ 1. บริษัทฯมีหน้าที่การบริหารการจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

ข้อ 2. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ 3. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ต และบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์ หรือวิธีการที่ส่งผลได้ เช่นกัน

ข้อ 4. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ 5. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ 6. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บอุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

ข้อ 7. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางบริษัทฯ อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากบริษัทฯก่อน

ข้อ 8. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กำหนดเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ 9. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ 10. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการสายงานระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ 11. บริษัทฯ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ 12. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากบริษัทฯ ก่อน

ข้อ 13. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

4. นโยบายความมั่นคงปลอดภัยของอีเมล์ (E-mail Policy)

ข้อ 1. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์(e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่บริษัทฯ

ข้อ 2. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ 3. ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ 4. ควรเปลี่ยนรหัสผ่าน (Password) ทุก 90 วัน

ข้อ 5. ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน (e-mail)

ข้อ 6. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นควรลงบันทึกออก (Logout) ทุกครั้ง

ข้อ 7. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

5. นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

ข้อ 1. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ 2.ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ 3. ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ 4. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ 5. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ 6. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

6. นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access control policy)

หมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ 1. บริษัทฯ กำหนดการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าในระบบสารสนเทศของหน่วยงาน จะต้องอนุญาตเป็นลายลักษณ์อักษรต่อผู้บัญชาการสำนักงาน

ข้อ 2. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ 3. ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ 4. ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งที่ผู้ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวดที่ 2 การบริหารจัดการเข้าถึงระบบสารสนเทศ

ข้อ 1. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของบริษัทฯ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ 2. ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ 3. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
2) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)
3) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)
4) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
5) กำหนดรายชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
6) ในกรณีมีความจำเป็นต้องใช้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์

พิเศษที่ได้ว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ 4. ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
5) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
6) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

7. นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

ข้อ 1. บริษัทฯ กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ 2. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้จัดการ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ 3. การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้จัดการ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

ข้อ 4. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ 5. ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายอย่างมีประสิทธิภาพดังต่อไปนี้

1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
2) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆได้
4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
5) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ
6) เลขที่ (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้
7) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
8) การใช้เครื่องมือต่างๆเพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ(System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ 6. ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (System Software)

ข้อ 7. บริษัทฯ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

1) ควรจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์(Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูลและผู้ดูแล ระบบไม่ได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย
2) ควรจัดกำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่นบันทึกเข้า-ออกระบบ บันทึกการพยายามเข้าระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง
3) ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ
4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ 8. บริษัทฯ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

1. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้จัดการ
2. มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
3. วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับอนุญาตจากผู้จัดการ
4. การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ
5. การเข้าใช้ระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

8. นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy)

1. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย
2. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ
3. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้แสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่าง ชัดเจน ข้อมูลที่สำรองควรเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ
4. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

9. นโยบายการรักษาความลับของข้อมูล (Confidentiality)

1. การจัดระดับข้อมูลสารสนเทศ (Information Classification)

บริษัทได้กำหนดให้มีการแบ่งระดับความปลอดภัยของข้อมูลองค์กร โดยคำนึงถึงระดับความเสี่ยงองค์กร ผลกระทบในการดำเนินธุรกิจ ความเสียหายที่ผู้มีส่วนได้ส่วนเสียอาจได้รับ ความเสียหายทางทรัพย์สินและชื่อเสียงในการดำเนินธุรกิจ ข้อมูลขององค์กรสามารถแบ่งออกตามระดับความสำคัญ 3 ระดับ ดังนี้

- ข้อมูลที่เผยแพร่ได้ (Public) เป็นข้อมูลที่มีเจตนาต้องการให้ลูกค้าหรือบุคคลภายนอกทราบ เช่น Catalogue และ Brochure ที่จัดทำออกมาเพื่อประชาสัมพันธ์ เป็นต้น
- ข้อมูลภายใน (Internal) เป็นข้อมูลสำหรับให้พนักงานขององค์กรใช้เท่านั้น และไม่มีเจตนาให้ภายนอกทราบ แต่ถ้าหากถูกนำไปเผยแพร่ออกไปสู่ผู้อื่นที่ไม่เกี่ยวข้อง อาจทำให้เกิดความเสียหายแก่องค์กร ลูกค้า หรือพนักงานได้ จึงต้องรักษาป้องกันมิให้รั่วไหล เช่น รายงานทุกรายงานจากระบบคอมพิวเตอร์ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล และงบประมาณขององค์กร เป็นต้น

ข้อมูลลับ (Confidential) เป็นข้อมูลที่สำคัญที่สุด หากถูกเผยแพร่ออกไปสู่ผู้อื่นที่ไม่เกี่ยวข้อง จะทำให้องค์กร ลูกค้า หรือพนักงาน เสื่อมเสียชื่อเสียง ได้รับการกล่าวโทษ หรือฟ้องร้อง หรือเกิดความเสียหายอย่างยิ่ง จึงต้องมีการระวังรักษาป้องกันอย่างเข้มงวด เช่น ข้อมูลเกี่ยวกับบริการใหม่ที่ยังไม่ถึงเวลาประกาศ ข้อมูลงบการเงินที่ยัง

ไม่ถึงเวลาประกาศ ข้อมูลการรวบรวมกิจการ หรือการเพิ่มทุนที่ยังไม่ถึงเวลาประกาศ และรหัสผ่านของระบบงานต่างๆ ข้อมูลการออกแบบ สูตรการผลิต เป็นต้น

2. การจัดการเกี่ยวกับข้อมูลข่าวสาร (Information Handling)

ข้อมูลถือเป็นทรัพย์สินขององค์กร พนักงานทุกคนมีหน้าที่ดูแลรักษาข้อมูลที่ตนเองดูแลรับผิดชอบอยู่ โดยให้พิจารณาการจัดการตามระดับความสำคัญของข้อมูล เพื่อลดความเสี่ยงต่อความเสียหายทางทรัพย์สิน และชื่อเสียงในการดำเนินธุรกิจการจัดชั้นความลับของสารสนเทศ (Information Classification) เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม มีข้อปฏิบัติ ดังนี้

2.1 ให้หน่วยงานจัดทำรายการสารสนเทศโดยระบุชื่อระบบสารสนเทศ คุณสมบัติ การจัดเก็บ

2.2 ให้หน่วยงานกำหนดชั้นความลับสารสนเทศ ได้แก่

1.) ไม่เป็นความลับ (Public)

2.) เป็นความลับของฝ่ายหรือแผนกไม่สามารถเผยแพร่ไปสู่พนักงานฝ่ายหรือแผนกอื่นได้ (Internal)

3.) เป็นความลับของตำแหน่งหรือกลุ่มตำแหน่งที่ตนบริหารจัดการอยู่เท่านั้น (Confidential)

2.3 กำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

การเข้าถึงข้อมูล และระบบสารสนเทศ จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้มีอำนาจตามที่ได้กำหนดในกระบวนการอนุมัติสิทธิ์การเข้าถึงข้อมูล และสามารถเข้าใช้ข้อมูลหรือระบบเฉพาะที่เกี่ยวข้องกับหน้าที่ของบุคคลนั้นๆ เท่านั้น ความปลอดภัยของข้อมูลและกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์

3. หน่วยงานที่เกี่ยวข้อง

3.1. ฝ่ายไอที

3.2. ฝ่ายที่ร้องขอ

3.3. ฝ่ายทรัพยากรบุคคล

4. หน้าที่ความรับผิดชอบ

4.1. รองกรรมการผู้จัดการ

4.1.1 อนุมัติแผนการทำนโยบายรักษาความปลอดภัยสารสนเทศ

4.1.2 อนุมัติแผนการบำรุงรักษาเครื่องคอมพิวเตอร์ประจำปี (FR-IT-02)

4.1.3 ตรวจสอบ และลงนามอนุมัติเครื่องคอมพิวเตอร์ใหม่ และยกเลิกเครื่องคอมพิวเตอร์ที่ไม่ใช้แล้ว

4.1.4 อนุมัติการขอสิทธิ์การใช้งานในระบบคอมพิวเตอร์

4.1.5 อนุมัติการใช้งาน Privilege Users ของระบบ รวมถึงการเข้าถึงระบบจากบุคคลภายนอก

4.1.6 อนุมัติแผนการดำเนินงานระยะยาวของฝ่ายไอที

4.2. ผู้จัดการฝ่ายไอที

4.2.1 อนุมัติแบบขอบริการงาน IT (FR-IT-01) ในกรณีต้องมีการจัดซื้อจัดจ้าง

4.2.2 ตรวจสอบแผนการทำนโยบายรักษาความปลอดภัย

4.2.3 ตรวจสอบแผนการบำรุงเครื่องคอมพิวเตอร์ประจำปี (FR-IT-02)

4.2.4 ตรวจสอบโปรแกรมในการสำรองข้อมูลแบบอัตโนมัติ

4.2.5 ตรวจสอบใบบันทึกรายงานตรวจเช็คระบบประจำวัน

4.2.6 ตรวจสอบแผนการดำเนินงานระยะยาวของฝ่ายไอที

4.2.7 ตรวจสอบการเข้าถึงของ Server

4.3. เจ้าหน้าที่ไอที

4.3.1 บริการผู้ใช้งานไอทีตามแบบขอบริการงาน IT (FR-IT-01)

4.3.2 จัดทำแผนและปฏิบัติงานตามแผนการบำรุงรักษาเครื่องคอมพิวเตอร์ประจำปี (FR-IT-02)

4.3.3 จัดทำและทบทวนบัญชีรายชื่อเครื่องคอมพิวเตอร์ และแผนผังการวางเครื่องคอมพิวเตอร์ที่มีผลต่อระบบคุณภาพทุกเครื่อง รวมถึงการต่ออายุเว็บไซต์ โฮสติ้ง ลิขสิทธิ์ต่างๆ

4.3.4 ทำการบำรุงเครื่องคอมพิวเตอร์ให้สามารถใช้ได้อย่างมีประสิทธิภาพ ตามแบบฟอร์มรายการตรวจซ่อมบำรุงเครื่องคอมพิวเตอร์ (FR-IT-03)

4.3.5 บันทึกผลลงในแบบฟอร์มรายการตรวจสอบซ่อมบำรุงเครื่องคอมพิวเตอร์(FR-IT-03)

4.3.6 รับใบแจ้งซ่อม แล้วทำการตรวจสอบ, ดำเนินการซ่อม, ประเมินผล และบันทึกลงประวัติเครื่อง

4.3.7 ทำการตรวจเช็คผลการสำรองข้อมูลอัตโนมัติ และลงบันทึกประจำวัน พร้อมนำเสนอรายงานผลให้ผู้จัดการฝ่ายไอทีตรวจสอบ

4.3.8 ทำการกู้คืนข้อมูลจาก File Server ให้กับ User หรือเมื่อเกิดเหตุจำเป็น

4.3.9 อนุมัติการเข้าถึงเครื่อง Sever

4.3.10 จัดทำแผนการทำนโยบายรักษาความปลอดภัย และแผนการดำเนินงานระยะยาวฝ่ายไอที

10. รายละเอียดการติดต่อบริษัทฯ

หากท่านมีข้อซักถามหรือข้อสงสัยประการใดเกี่ยวกับนโยบายความมั่นคงและความปลอดภัยด้านเทคโนโลยีสารสนเทศโปรดติดต่อบริษัทฯ หรือเจ้าหน้าที่เทคโนโลยีสารสนเทศของบริษัทฯ ที่

บริษัท บางกอก เฮลท์ กรุ๊ป จำกัด
เลขที่ 160/15-17 ถนนจอมสุรางค์ยาตร์
ตำบลในเมือง อำเภอเมือง จังหวัดนครราชสีมา 30000
โทรศัพท์ : 044-254127
เจ้าหน้าที่เทคโนโลยีสารสนเทศ
E-mail : IT@bangkokhealthgroup.com
โทรศัพท์ : 095-6132114

จึงประกาศให้ทราบโดยทั่วกัน

.....
(นางธนกาญจน์ วิษณุโยธิน)
ประธานคณะกรรมการ