



ประกาศมหาวิทยาลัยราชภัฏนครสวรรค์  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏนครสวรรค์ เป็นไปตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๑(๑) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ ประกอบ มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และหนังสือสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ ๐๒๐๙/ว๒๙๒๗ ลงวันที่ ๑๓ ตุลาคม ๒๕๕๔ เรื่อง ขอความร่วมมือดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศมหาวิทยาลัยราชภัฏนครสวรรค์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร ความดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยราชภัฏนครสวรรค์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร”

ข้อ ๒ ประกาศนี้ ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวัน นับแต่วันประกาศใช้ประกาศฉบับนี้เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยราชภัฏนครสวรรค์

“หน่วยงาน” หมายถึง คณะ สำนัก สถาบัน ศูนย์ หรือหน่วยงานอื่นที่มีฐานะเทียบเท่าคณะ ที่เป็นหน่วยงานภายในมหาวิทยาลัยราชภัฏนครสวรรค์

“ผู้ใช้งาน” หมายถึง บุคลากร นักศึกษา ลูกจ้าง ผู้ดูแลระบบหรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สินทรัพย์ของมหาวิทยาลัย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยราชภัฏนครสวรรค์ หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัยราชภัฏนครสวรรค์

“สินทรัพย์” หมายถึง เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาขึ้นหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

“เครื่องคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ห้องคอมพิวเตอร์แม่ข่าย” หมายถึง สถานที่ติดตั้งอุปกรณ์แม่ข่ายหรืออุปกรณ์เครือข่ายของมหาวิทยาลัยภายในมหาวิทยาลัย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง ความสามารถในการเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ในการอ่าน สร้าง สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง ความมั่นคงและความปลอดภัยในบริบทของการรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของระบบสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์ โดยมีเป้าหมายเพื่อปกป้องสินทรัพย์ของมหาวิทยาลัยจากเหตุการณ์หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ซึ่งอาจทำให้เกิดความเสียหายต่อสินทรัพย์ของมหาวิทยาลัย

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพการใช้งาน การให้บริการเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์ ที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“เครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์” หรือเรียกอีกนามหนึ่ง “เครือข่าย NSRUNet” หมายถึง ระบบเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ฯ โดยมีวัตถุประสงค์การใช้งานเพื่อการบริหารงาน การบริการวิชาการการศึกษาและงานวิจัยที่เป็นพันธกิจของมหาวิทยาลัย

“ผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์” หมายถึง บุคลากรที่ได้รับมอบหมายจากมหาวิทยาลัยเพื่อปฏิบัติงานให้ดูแลบริหารจัดการระบบเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์ ให้พร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ปฏิบัติงานระบบสารสนเทศ” หมายถึง บุคลากรที่ได้รับมอบหมายจากหน่วยงาน เพื่อทำการป้อนข้อมูล และแก้ไขข้อมูลของระบบสารสนเทศของมหาวิทยาลัย

“เครือข่ายย่อย” หมายถึง อุปกรณ์ต่อพ่วงต่าง ๆ รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ต่าง ๆ ภายในเครือข่ายสารสนเทศมหาวิทยาลัยราชภัฏนครสวรรค์ ตลอดจนถึงโปรแกรมและข้อมูลต่าง ๆ

“ผู้ดูแลระบบเครือข่ายย่อย” หมายถึง บุคลากรหรือลูกจ้างได้รับมอบหมายจากหัวหน้าหน่วยงาน เพื่อปฏิบัติงานให้ระบบเครือข่ายของหน่วยงานพร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ใช้บริการเครือข่าย” หมายถึง บุคคล หน่วยงานที่ต่อเชื่อมและรับบริการจากเครือข่ายสารสนเทศมหาวิทยาลัย

“ผู้บริหารระดับสูงสุด” หมายถึง อธิการบดีมหาวิทยาลัยราชภัฏนครสวรรค์

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายถึง ผู้ที่ได้รับการแต่งตั้งจากมหาวิทยาลัยราชภัฏนครสวรรค์ ให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัยราชภัฏนครสวรรค์ เพื่อทำหน้าที่ในการกำหนด ตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“ผู้ตรวจสอบภายใน” หมายถึง บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัย เพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“ผู้ตรวจสอบจากภายนอก” หมายถึง เป็นบุคคลภายนอกที่มีความรู้ ความสามารถทางด้านเทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“บทลงโทษ” หมายถึง บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๖ -๑๔

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร บุคลากรทางด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏนครสวรรค์

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัยราชภัฏนครสวรรค์

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้ง มีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๗. บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทำปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ อันได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙. ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐. ควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการวางเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑. ควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชัน และสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึง

สารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๒. จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทาง ต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) ปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔. ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ดังนี้

(๑) ระดับนโยบาย

๑.๑ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบในการกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏนครสวรรค์ โดยมีหน้าที่กำกับ ดูแล รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนว

ปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้การสนับสนุนและส่งเสริมการดำเนินงานด้านสารสนเทศอย่างมีประสิทธิภาพ

๑.๒ ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทำหน้าที่ติดตาม กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงานผู้รับผิดชอบระดับปฏิบัติงาน กำกับดูแลให้มีการปฏิบัติ และดำเนินการตามประกาศ ฉบับนี้

(๒) ระดับปฏิบัติงาน ได้แก่

๒.๑ ผู้ดูแลรับผิดชอบเครือข่ายของมหาวิทยาลัยราชภัฏนครสวรรค์ ในตำแหน่ง นักวิชาการคอมพิวเตอร์ รับผิดชอบงานพัฒนาระบบเครือข่ายและสารสนเทศ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตาม การปฏิบัติงานตามแผน การบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๒.๑.๑ ควบคุมการเข้า - ออก ห้องคอมพิวเตอร์แม่ข่าย (Server) ตามการกำหนด สิทธิการเข้าถึง คอมพิวเตอร์แม่ข่าย (Server)

๒.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยราชภัฏนครสวรรค์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๒.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบการเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการในมหาวิทยาลัยราชภัฏนครสวรรค์

๒.๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๒.๑.๕ แก้ไขปัญหาที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๒.๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

๒.๑.๗ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึง ระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๒.๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบฐานข้อมูลทั้งหมดที่ให้บริการให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๒.๑.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของระบบ

๒.๑.๑๑ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาาระบบความมั่นคง ปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๑๒ รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

๒.๑.๑๓ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Back up and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๑.๑๔ บริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) ระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๒.๒ ผู้ดูแลระบบ จากบริษัทที่จัดจ้างให้ดูแลระบบเครือข่ายและคอมพิวเตอร์ รับผิดชอบ ดังนี้

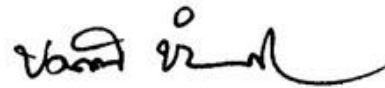
๒.๒.๑ แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

๒.๒.๒ กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

๒.๒.๓ รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูลและสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

๒.๒.๔ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยราชภัฏนครสวรรค์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง (แก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายในองค์กร)

ประกาศ ณ วันที่ ๑๕ กรกฎาคม พ.ศ. ๒๕๕๘



(ผู้ช่วยศาสตราจารย์บัญญัติ ชำนาญกิจ)  
อธิการบดีมหาวิทยาลัยราชภัฏนครสวรรค์