ประกาศ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร
เรื่อง นโยบายความมั่นคงปลอดภัยทางด้านระบบฐานข้อมูลของคณะวิทยาศาสตร์

ข้อมูลสารสนเทศ เป็นสินทรัพย์สำคัญของหน่วยงาน ที่ต้องดูแลบำรุงรักษา และป้องกันอย่างดี ปัจจุบันคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร มีการนำคอมพิวเตอร์มาประยุกต์ใช้เพื่อให้เกิดประสิทธิภาพต่อการทำงานในทุกหน่วยงานของคณะโดยมีการเชื่อมต่อเครือข่ายภายในและภายนอก ซึ่งคอมพิวเตอร์เหล่านี้อาจถูกโจมตี และเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรืออาจจะมีการติดไวรัสคอมพิวเตอร์ หรือโปรแกรมประเภทไม่พึงประสงค์ต่างๆ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศเหล่านี้จึงได้กำหนดนโยบายความมั่นคงปลอดภัยระบบฐานข้อมูล โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงาน และลดความเสี่ยงด้านความปลอดภัย จากการบริหารจัดการระบบข้อมูลที่มีการรักษาความลับ ความถูกต้องแท้จริง และสามารถพร้อมใช้เสมอเพื่อให้เกิดประสิทธิภาพต่อการทำงานสูงสุด อาศัยอำนาจตามความในมาตรา ๒๖ แห่งพระราชบัญญัติมหาวิทยาลัยนเรศวร พ.ศ. ๒๕๓๓ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร จึงได้กำหนดนโยบายด้านความมั่นคงปลอดภัยทางด้านระบบฐานข้อมูลให้เป็นไปอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้นได้อย่างรวดเร็ว ดังรายละเอียดที่แนบท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ 3 กรกฎาคม พ.ศ. 2552

(รองศาสตราจารย์ ดร.ชยันต์ บุณยรักษ์)
คณบดีคณะวิทยาศาสตร์

นโยบายความมั่นคงปลอดภัยทางด้านระบบฐานข้อมูลของคณะวิทยาศาสตร์

ข้อมูลสารสนเทศ เป็นสินทรัพย์สำคัญของหน่วยงาน ที่ต้องดูแลบำรุงรักษา และป้องกันอย่างดี ปัจจุบันคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร มีการนำคอมพิวเตอร์มาประยุกต์ใช้เพื่อให้เกิดประสิทธิภาพต่อการทำงานในทุกหน่วยงานของคณะ โดยมีการเชื่อมต่อเครือข่ายภายในและภายนอก ซึ่งคอมพิวเตอร์เหล่านี้อาจถูกโจมตี และเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรืออาจจะมีการติดไวรัสคอมพิวเตอร์ หรือโปรแกรมประเภทไม่พึงประสงค์ต่างๆ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศเหล่านี้ จึงได้กำหนดนโยบายความมั่นคงปลอดภัยระบบฐานข้อมูล โดยการนำเทคโนโลยีความปลอดภัยที่สำคัญมาใช้ในองค์กร เพื่อช่วยในการทำงาน และลดความเสี่ยงด้านความปลอดภัยจากการบริหารจัดการระบบข้อมูลที่มีการรักษาความลับ ความถูกต้องแท้จริง และสามารถพร้อมใช้เสมอ เพื่อให้เกิดประสิทธิภาพต่อการทำงานสูงสุด รายละเอียดของนโยบายฯ มีดังนี้

บทที่ 1 คำนิยาม

"**เทคโนโลยีสารสนเทศ** (IT)" หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

"**การรักษาความลับ** (Confidentiality)" หมายถึง ให้บุคคลผู้มีสิทธิเท่านั้นสามารถเข้าถึงและเรียกดูข้อมูลได้ ต้องมีการควบคุมการเข้าถึง ข้อมูลเป็นความลับต้องไม่เปิดเผยกับผู้ไม่มีสิทธิ

"**ความถูกต้องแท้จริง** (Integrity)" หมายถึง มีเกราะป้องกันความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล และวิธีการประมวลผล ต้องมีการควบคุมความผิดพลาด ไม่ให้ผู้ไม่มีสิทธิมาเปลี่ยนแปลงแก้ไขได้

"**ความสามารถพร้อมใช้เสมอ** (Availability)" หมายถึง ให้บุคคลผู้มีสิทธิเท่านั้นเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ระบบล้มเหลว มีสมรรถภาพในการทำงานต่อเนื่อง ไม่ให้ผู้ไม่มีสิทธิมาทำให้ระบบหยุดการทำงาน

"**คณะกรรมการความมั่นคงปลอดภัยทางด้านระบบฐานข้อมูล**" หมายถึง คณะกรรมการที่คณะวิทยาศาสตร์แต่งตั้งเพื่อพิจารณากำหนดนโยบายความมั่นคงปลอดภัยทางด้านระบบฐานข้อมูล

"**ผู้ใช้** (User)" หมายถึง บุคลากรภายในคณะวิทยาศาสตร์ที่มีบัญชีคอมพิวเตอร์ที่ออกโดยหน่วยระบบเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และ/หรือ บุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครือข่าย

“**ผู้ดูแลระบบ** (System Administrator)” หมายถึง ผู้ซึ่งได้รับมอบหมายจากผู้บริหารหรือจากหน่วยระบบเทคโนโลยีสารสเทศ คณะวิทยาศาสตร์ ให้ทำหน้าที่ดูแลเครื่องคอมพิวเตอร์และเครือข่ายให้บริการได้อย่างมีเสถียรภาพ

“**เครื่องคอมพิวเตอร์ลูกข่าย**” หมายความถึง เครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งเป็นทรัพย์สินของคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ที่ได้จัดสรรให้บุคลากรใช้งาน ซึ่งแบ่งเป็นสองประเภท คือ เครื่องคอมพิวเตอร์ประจำตัวและเครื่องคอมพิวเตอร์ให้บริการ

“**เครื่องคอมพิวเตอร์แม่ข่าย**” หมายความถึง เครื่องคอมพิวเตอร์ที่มีไว้สำหรับรองรับระบบฐานข้อมูล และเว็บแอพลิเคชั่น ของคณะวิทยาศาสตร์

“**เครื่องคอมพิวเตอร์ส่วนตัว**” หมายความถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและ/หรือเครื่องคอมพิวเตอร์แบบกระเป๋า (Notebook) ที่ผู้ใช้นำมาเอง

“**โปรแกรมประเภทไม่พึงประสงค์** (Malware)” หมายความว่า โปรแกรมมุ่งร้ายที่มาในรูปแบบต่างๆ ไม่ว่าจะเป็นระบบโปรแกรมให้ความช่วยเหลือวินโดวส์ (ActiveX หรือ Java Applet) ที่มากับการใช้งานโปรแกรมบราวเซอร์ โดยไม่ได้รับการติดตั้งโปรแกรมแก้ไขข้อผิดพลาด (Patch) ตลอดจนแฝงมากับโปรแกรมที่แจกจ่ายให้ใช้งาน (Shareware, Freeware) หรือโปรแกรมอำนวยความสะดวก (Utility) หรือโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์แต่ละเครื่องมีการเชื่อมโยงกันโดยตรง (Peer to Peer) ที่นิยมใช้ในการดาวน์โหลดเพลง หรือภาพยนตร์ ผ่านทางอินเทอร์เน็ตหรือมาในรูปแฟ้มข้อมูลบีบอัด (Zip File) หรือมีการปลอมแปลงชื่อผู้ส่ง ปลอมแปลงจดหมายอิเล็กทรอนิกส์ (E-mail) ซึ่งมีเนื้อความและชื่อจดหมายอิเล็กทรอนิกส์ ตลอดจนชื่อผู้ส่งที่ปลอมแปลงมาดูแล้วน่าเชื่อถือ

“**การพิสูจน์ฝ่าย** (Authentication)” คือการตรวจสอบและการพิสูจน์สิทธิของการขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิ สำหรับอุปกรณ์ไอที รวมถึงแอพลิเคชั่นทั้งหลาย

“**การพิสูจน์สิทธิ์** (Authorization)” หมายถึงการตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพลิเคชั่น นั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

“**การเก็บสำรองข้อมูล** (Data backup)” หมายถึง ในระหว่างการเก็บสำรอง สำเนาของชุดข้อมูลปัจจุบันจะถูกสร้างขึ้นมา เพื่อป้องกันการสูญหายของขอ้มมูล

“**การปกป้องข้อมูล** (Data protection)” หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

“**การรักษาความมั่นคงปลอดภัยของข้อมูล** (Data security)” หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้

"**การประเมินความเสี่ยง หรือการวิเคราะห์ความเสี่ยง** (Risk assessment or analysis)" ของระบบสารสนเทศ หมายถึง การตรวจสอบโอกาสของผลลัพธ์ใดๆ ที่ไม่พึงประสงค์ต่อระบบฯ และผลเสียที่อาจจะเกิดขึ้นตามมาได้

"**นโยบายด้านความมั่นคงปลอดภัย** (Security policy)" หมายถึงนโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการขององค์กร รายละเอียดของวิธีการด้านความมั่นคงปลอดภัยมักจะอธิบายแยกไว้ในรายงานต่างหาก

บทที่ 2 การจัดลำดับชั้นความมั่นคงปลอดภัยของระบบฐานข้อมูลลำดับชั้นความมั่นคงปลอดภัยของระบบฐานข้อมูลแบ่งเป็น 3 ระดับ คือ

2.1 ระดับที่ 1 (ความมั่นคงปลอดภัยขั้นสูง) คือ ระบบฐานข้อมูลที่ใช้ปฏิบัติงานและมีการจัดเก็บหรือบันทึกข้อมูลที่มีความสำคัญ หากข้อมูลเสียหายจะส่งผลกระทบต่อการดำเนินงานของคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ได้แก่ ระบบฐานข้อมูลด้านการเงิน การบัญชี ระบบฐานข้อมูลบุคคลากร ระบบฐานข้อมูลงานสารบรรณและงานพัสดุ หรืองานอื่น ใดที่จะกำหนดเพิ่มเติมในภายหลัง

2.2 ระดับที่ 2 (ความมั่นคงปลอดภัยขั้นปานกลาง) คือ ระบบฐานข้อมูลที่ปฏิบัติงานเฉพาะด้าน เป็นระบบฐานข้อมูลที่ใช้สำหรับการทดสอบงาน ได้แก่ ระบบฐานข้อมูลเว็บไซต์คณะวิทยาศาสตร์ เว็บไซต์ของภาควิชา ระบบฐานข้อมูลที่จัดทำให้กับหน่วยงานวิชาการ กิจการนิสิต งานห้องปฏิบัติการ

2.3 ระดับที่ 3 (ความมั่นคงปลอดภัยขั้นพื้นฐาน) คือ ระบบฐานข้อมูลที่จัดทำขึ้นมาเพื่อใช้ในงานกิจกรรมทั่วไปที่คณะวิทยาศาสตร์จัดขึ้น

บทที่ 3 ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบฐานข้อมูล

3.1 ระบบฐานข้อมูลแต่ละระบบจะต้องมีชื่อผู้รับผิดชอบที่ได้รับมอบหมายจากเจ้าหน้าที่ดูแลระบบอย่างชัดเจน

3.2 ระบบฐานข้อมูลทุกระบบต้องมีรหัสผ่านประจำระบบสำหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

3.3 เครื่องแม่ข่ายที่รองรับระบบฐานข้อมูลทุกระบบที่ใช้ในคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวรต้องมีการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus , AntiSpyware) และโปรแกรมป้องกันการบุกรุก (Firewall) เป็นไปตามข้อกำหนดของหน่วยระบบเทคโนโลยีสารสนเทศ

3.4 ระบบฐานข้อมูลทุกระบบควรมีการป้องกันโดยใช้รหัสผ่าน (Password) ในระดับของผู้ใช้ทั่วไป และผู้ดูแลระบบ เพื่อตรวจสอบการเข้าใช้งานเบื้องต้นของระบบ

3.5 เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องควรลงโปรแกรมสำหรับการบริหารจัดการเครื่องคอมพิวเตอร์ เพื่อป้องกันการติดตั้งโปรแกรมหรือการแก้ไขค่าติดตั้งประจำเครื่องเช่น ค่าหมายเลขในการเชื่อมต่ออินเทอร์เน็ต (IP Address) หรือเปลี่ยนแปลงสิทธิการใช้เครื่อง เป็นต้น

3.6 เครื่องคอมพิวเตอร์แม่ข่ายควรติดตั้งระบบโปรแกรมพักหน้าจอ(Screen Saver) โดยกำหนดรหัสในการเข้าใช้

3.7 ห้ามผู้ใช้ระบบฐานข้อมูลที่ไม่ได้รับอนุญาตให้เข้าใช้งานระบบฐานข้อมูลที่มีความมั่นคงปลอดภัยของฐานข้อมูลระดับที่ 1 โดยเด็ดขาด หากมีความจำเป็นให้ผู้ใช้อื่นปฏิบัติงาน ผู้ใช้ประจำระบบฐานข้อมูลจะต้องอนุญาตและรับผิดชอบในการใช้งานระบบ

3.8 การเข้าถึงข้อมูลจะถูกจำกัดโดยผู้ดูแลระบบ ห้ามมิให้ผู้ใช้งานเข้าถึงข้อมูลที่ไม่อนุญาต

3.9 การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายจะเป็นความรับผิดชอบของผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย

3.10 ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานในความมั่นคงปลอดภัยของระบบฐานข้อมูลระดับที่หนึ่ง

3.11 การใช้งานเครื่องคอมพิวเตอร์ส่วนตัวควรมีการดำเนินการตามข้อ 4.1เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในระบบส่วนราชการ

บทที่ 4 ข้อกำหนดการใช้งานทั่วไป

4.1 ข้อกำหนดการใช้งานระบบฐานข้อมูลสำหรับผู้ใช้ทั่วไป

4.1.1 ห้ามมิให้มีการเปิดระบบแชร์แฟ้มข้อมูลหรือโฟลเดอร์ของเครื่องคอมพิวเตอร์แม่ข่ายให้กับผู้ใช้ระบบฐานข้อมูลทั่วไป ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบเป็นรายกรณี

4.1.2 ห้ามมิให้ทำการดาวน์โหลดไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็นและไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้งานด้านเครือข่ายอย่างหนาแน่น

4.1.3 หากระบบฐานข้อมูลไม่สามารถทำงานได้ตามปกติ ผู้ใช้งานทั่วไปสามารถแจ้งผู้ดูแลระบบเพื่อแก้ไขปัญหาได้ ห้ามมิให้ผู้ใช้งานทั่วไปติดตั้งปรับแก้ และเปลี่ยนแปลงข้อมูลในระบบด้วยตนเอง ยกเว้นได้รับอนุญาตจากผู้ดูและระบบเป็นรายกรณี

4.1.4 ผู้ใช้งานทั่วไปต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเมื่อมีการแจ้งให้เปลี่ยนรหัสผ่านเข้าสู่ระบบ

4.1.5 ห้ามติดตั้งซอฟต์แวร์อื่นใดที่เกี่ยวข้องกับการทำงานของระบบฐานข้อมูล หากจำเป็นต้องติดตั้งให้ติดต่อขออนุญาตจากผู้ดูแลระบบ

4.1.6 ให้ตรวจสอบเครื่องคอมพิวเตอร์ลูกข่ายว่ามีโปรแกรมไวรัสคอมพิวเตอร์ หรือโปรแกรมประเภทไม่พึงประสงค์ (Malware) ในเครื่องคอมพิวเตอร์ลูกข่ายหรือไม่อย่างน้อยสัปดาห์ละหนึ่งครั้ง

4.2 ข้อกำหนดการใช้งานของผู้ดูแลระบบ

4.2.1 กำหนดรหัสผ่านให้กับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบจะมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

4.2.2 ติดตั้งซอฟต์แวร์ต่างๆ ที่จำเป็นต่อการใช้งานให้เหมาะสมต่อการใช้งานในแต่ละระดับ

4.2.3 ทำการปรับปรุง (Update) โปรแกรมต่างๆ เช่น Windows server 2003, Antivirus และAntiSpyware เพื่อให้โปรแกรมมีคุณสมบัติที่ทันสมัยและเป็นปัจจุบันอยู่เสมอ

4.2.4 ทำการปรับปรุง (Update) ฐานข้อมูลไวรัสคอมพิวเตอร์ทุกสัปดาห์ให้เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอยู่ในสภาพพร้อมใช้และปราศจากโปรแกรมที่ไม่พึงประสงค์

4.2.5 ทำการตรวจหา (Scan) ไวรัสคอมพิวเตอร์และโปรแกรมไม่พึงประสงค์ (Malware) ในเครื่องแม่ข่ายเป็นประจำทุกสัปดาห์

4.2.6 ปิดระบบการให้บริการของระบบปฏิบัติการบางส่วนที่อาจทำให้เป็นช่องทางในการเข้าจู่โจมของผู้บุกรุก และระบบการให้บริการที่ไม่เกี่ยวข้องกับการทำงานของผู้ใช้ทั่วไปเช่น ปิดการให้บริการระบบฐานข้อมูลในปฏิบัติการ Windows Server บางส่วน

4.2.7 ให้ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อคณะกรรมการด้านความมั่นคงปลอดภัยระบบฐานข้อมูลของคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เช่น มีการติดไวรัสคอมพิวเตอร์ ที่เครื่องคอมพิวเตอร์แม่ข่ายในระดับความมั่นคงทุกระดับทันทีที่เกิดเหตุการณ์ขึ้น

4.2.8 ให้ผู้ดูแลระบบบันทึกรายงานผลการปฏิบัติงานเสนอต่อคณะกรรมการด้านความมั่นคงปลอดภัยระบบฐานข้อมูลของคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร เมื่อทำการตรวจซ่อม บำรุงรักษาเครื่องคอมพิวเตรอ์แม่ข่ายประจำทุกเดือน

4.2.9 ให้ผู้ดูแลระบบบันทึกและรายงานผู้ใช้ที่ฝ่าฝืนแนวนโยบายเกี่ยวกับการใช้งานระบบฐานข้อมูลของคณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวรต่อผู้บริหารคณะ

วิทยาศาสตร์เพื่อเสนอให้คณะกรรมการความมั่นคงปลอดภัยระบบฐานข้อมูลของคณะวิทยาศาสตร์ พิจารณาเสนอผู้บริหาร คณะวิทยาศาสตร์ดำเนินการตามควรแก่กรณีต่อไป

4.2.10 ผู้ดูแลระบบประจำเครื่องคอมพิวเตอร์แม่ข่ายมีหน้าที่สำรองข้อมูล และดูแลรักษาเครื่องคอมพิวเตอร์ให้ใช้งานได้ตามปกติ

4.2.10.1 ระบบฐานข้อมูลที่มีความมั่นคงปลอดภัยระดับที่ 1 ให้สำรองข้อมูลทุกวันโดยผู้ดูแลระบบ

4.2.10.2 ระบบฐานข้อมูลที่มีความมั่นคงปลอดภัยระดับที่ 2 และ 3 ให้สำรองข้อมูลเป็นประจำทุกเดือน

4.2.11 ในกรณีที่ข้อมูลเกิดความเสียหาย ให้ผู้ดูแลระบบฐานข้อมูลกู้ข้อมูลกลับคืนมา ทั้งนี้หากระบบฐานข้อมูลที่มีความมั่นคงปลอดภัยระดับที่ 1 จะต้องดำเนินการโดยผู้ดูแลระบบอย่างรวดเร็ว

4.2.12 รายงานสิ่งผิดปกติที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายต่อผู้บริหาร

บทที่ 5 การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control) โดยมีระดับวิธีการ 3 วิธีคือ

5.1 การควบคุมจากระบบภายในของซอฟต์แวร์ (Internal Program Control) คือการที่ โปรแกรมนั้นได้มีการควบคุมสิทธิการเข้าถึง และสิทธิในการใช้ข้อมูลภายในระบบฐานข้อมูล ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลภายในระบบเอง

5.2 การควบคุมความปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) คือการควบคุมสิทธิการเข้าถึงและการใช้ข้อมูลในส่วนต่าง ๆ ภายในระบบคอมพิวเตอร์แม่ข่ายของผู้ดูแลระบบ และจำแนกแตกต่างจากผู้ใช้คนอื่น ๆ

5.3 การควบคุมและการออกแบบโปรแกรม (Development Control) คือการควบคุมตั้งแต่การออกแบบ การทดสอบก่อนการใช้งานจริงในระบบฐานข้อมูล

บทที่ 6 การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control)

โดยเลือกใช้เทคโนโลยีทางด้านฮาร์ดแวร์ ที่สามารถควบคุมการเข้าถึง และป้องกันการทำงานผิดพลาด ด้วยอุปกรณ์ภายในตัวเองของเครื่องคอมพิวเตอร์แม่ข่าย

บทที่ 7 การใช้นโยบายในการควบคุม (Policies)

โดยมีการประกาศใช้นโยบาย และการปรับปรุงนโยบายให้มีการทำงานสอดคล้องกับการดำเนินงานและสภาพแวดล้อมที่เปลี่ยนแปลง โดยมีผลบังคับใช้ทั้งองค์กร

บทที่ 8 การป้องกันทางกายภาพ (Physical Control)

การมีมาตรการการเข้าถึงหน่วยเทคโนโลยีสารสนเทศ และเครื่องคอมพิวเตอร์ที่สำคัญ ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย จะสามารถเข้าถึงได้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น (Authorization) รวมทั้งมีระบบสำรองข้อมูลอย่างสม่ำเสมอ โดยมีการกำหนดวัน เวลา ในการทำการสำรองข้อมูลที่จำเป็นต่อระบบสารสนเทศของคณะวิทยาศาสตร์