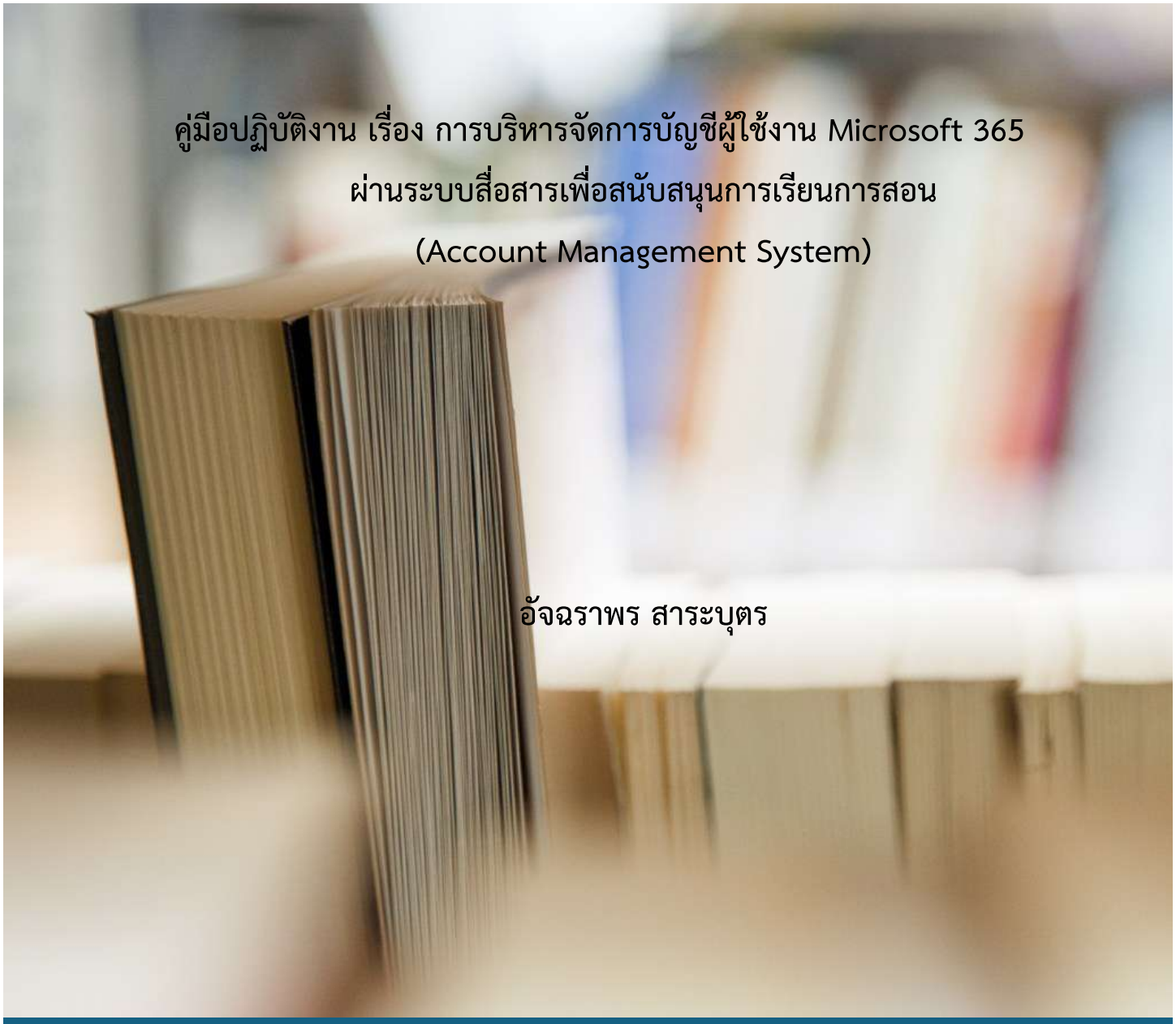


คู่มือปฏิบัติงาน เรื่อง การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน (Account Management System)

อัจฉราพร สาระบุตร

ส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย
สำนักเทคโนโลยีดิจิทัลและสารสนเทศ
สถาบันบัณฑิตพัฒนบริหารศาสตร์

คำนำ

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ มีหน้าที่ในการให้บริการด้านเทคโนโลยีต่างๆ รวมไปถึงการให้บริการบัญชีผู้ใช้งาน Microsoft 365 สำหรับนักศึกษา บุคลากร อาจารย์พิเศษ บัญชีอีเมลกลางสำหรับหน่วยงาน หรือหลักสูตร ซึ่งบัญชีผู้ใช้งาน Microsoft 365 นั้นเป็นบัญชีอีเมลหลักของสถาบันที่นอกจากจะใช้สำหรับรับ-ส่งอีเมลแล้ว ยังใช้สำหรับการเรียนการสอนแบบออนไลน์ รวมทั้งใช้ยืนยันตัวตนในการเข้าใช้งานระบบเครือข่ายหลัก และบริการสารสนเทศต่างๆของสถาบันเป็นต้น จึงมีความจำเป็นอย่างยิ่งที่จะต้องบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ให้เป็นไปด้วยความถูกต้อง รวดเร็วเพื่อตอบสนองความต้องการการใช้งานในปัจจุบัน

คู่มือปฏิบัติงานการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System) ฉบับนี้จะแสดงให้เห็นถึงกระบวนการในการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ตั้งแต่การสร้างบัญชีผู้ใช้งาน การแก้ไขข้อมูล การยกเลิกบัญชีผู้ใช้งาน รวมทั้งการแก้ไขปัญหาที่เกี่ยวกับบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System)

ผู้จัดทำหวังว่าคู่มือฉบับนี้จะเป็นประโยชน์ต่อผู้อ่านไม่มากก็น้อย ซึ่งผู้อ่านสามารถนำคู่มือนี้ไปศึกษา ต่อยอด หรือปรับปรุงกระบวนการปฏิบัติต่าง ๆ ให้มีประสิทธิภาพมากยิ่งขึ้น

นางอัจฉราพร สาระบุตร
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กุมภาพันธ์ 2568

สารบัญ

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

Microsoft 365 เดิมชื่อ Office 365 เป็นบริการจากบริษัท Microsoft ที่รวบรวมโปรแกรมและเครื่องมือต่างๆที่ช่วยในการทำงาน เช่น โปรแกรมด้านเอกสาร Microsoft Office (Microsoft Word, Excel, PowerPoint) รวมทั้งโปรแกรมที่ช่วยอำนวยความสะดวกในการทำงานร่วมกัน และสามารถทำงานพร้อมๆกันในทีมงาน หรือองค์กร เช่น Microsoft Sharepoint , Microsoft Team , บริการการจัดเก็บข้อมูลบนคลาวน์โดย OneDrive ผู้ใช้งานไม่ต้องกังวลในเรื่องเวอร์ชั่นของโปรแกรมที่ใช้งานเนื่องจาก Microsoft จะมีการปรับปรุงเวอร์ชั่นให้เป็นเวอร์ชั่นใหม่โดยอัตโนมัติ และมีการพัฒนาโปรแกรมต่างๆเพื่อให้บริการตลอดเวลา ทำให้การทำงานมีประสิทธิภาพมากยิ่งขึ้น (ที่มา : เว็บไซต์ https://support.microsoft.com/)

สถาบันได้นำ Microsoft 365 มาใช้งานเมื่อปีพ.ศ. 2560 โดยพิจารณาถึงซอฟต์แวร์ที่มีความเป็นมาตรฐานสากล เหมาะสมกับการใช้งานและสิ่งสำคัญคือต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามพระราชบัญญัติลิขลิทธิ์ พ.ศ. 2537 ทั้งนี้การใช้งาน Microsoft 365 ในช่วงเริ่มต้นยังไม่ค่อยได้รับความนิยมเนื่องจากยังสามารถทำงาน และจัดการการเรียนการสอนที่สถาบันได้ จนกระทั่งในปี พ.ศ. 2563 ที่มีการระบาดของ COVID-19 สถาบันได้ปรับเปลี่ยนรูปแบบการเรียนการสอน และการทำงานของบุคลากรให้สอดคล้องกับสถานการณ์ และสามารถดำเนินการในการเรียนการสอนได้โดยใช้ Microsoft 365 เพราะมีโปรแกรมและเครื่องมือต่างๆมากมายที่อำนวยความสะดวก และตอบโจทย์การทำงาน ทำให้การเรียนการสอนของสถาบันเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ นักศึกษาและบุคลากรได้เล็งเห็นถึงความสำคัญทำให้การใช้งาน Microsoft 365 ได้รับความนิยมมากยิ่งขึ้น

ปัจจุบันนักศึกษา บุคลากร หน่วยงานต่างๆของสถาบัน รวมทั้งอาจารย์พิเศษมีความจำเป็นต้องใช้งานบัญชีผู้ใช้งาน Microsoft 365 ของสถาบันเพื่อใช้ในการเรียนการสอน การประชุม รวมทั้งกิจกรรมต่างๆที่จัดในรูปแบบออนไลน์ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการบริหารจัดการบัญชีเพื่อให้ผู้ใช้งานสามารถเข้าใช้บริการต่างๆได้ทันต่อความต้องการ โดยระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System) รองรับการสร้าง และการยกเลิกบัญชีผู้ใช้งาน การบริหารจัดการกลุ่มของบริการประเภทต่างๆ การกำหนดสิทธิการใช้งานในแต่ละบัญชีผู้ใช้งาน หากไม่มีบัญชีผู้ใช้งาน Microsoft 365 การดำเนินการกิจกรรมต่างๆของสถาบันอาจล่าช้า หรือไม่สามารถดำเนินการได้ ทำให้การบริหารงานด้านต่างๆไม่บรรลุตามเป้าหมายที่กำหนดไว้

จากความเป็นมาและความสำคัญดังกล่าว จึงเป็นเหตุให้จัดทำคู่มือปฏิบัติงาน เรื่อง การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน (Account Management System) ขึ้น คู่มือฉบับนี้จะแสดงถึงการบริหารจัดการบัญชีผู้ใช้งานประเภทต่างๆ เพื่อให้ผู้ดูแลระบบและผู้เกี่ยวข้องกับระบบ สามารถนำไปศึกษาและปฏิบัติใช้งานได้

1.2 วัตถุประสงค์

1. เพื่อจัดทำคู่มือการบริหารจัดการบัญชีผู้ใช้งานผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System) สำหรับผู้ปฏิบัติงาน
2. เพื่อสร้างแนวปฏิบัติที่เป็นมาตรฐานสำหรับการบริหารจัดการบัญชีผู้ใช้งานผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System)
3. เพื่อเผยแพร่องค์ความรู้ในการบริหารจัดการบัญชีผู้ใช้งานการบริหารจัดการบัญชีผู้ใช้งานผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System)

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1. บุคลากรของสำนักเทคโนโลยีดิจิทัลและสารสนเทศสามารถใช้คู่มือในการปฏิบัติงานการบริหารบัญชีผู้ใช้งานที่ถูกต้องตามกระบวนการและกฎระเบียบ ป้องกันความผิดพลาดที่อาจเกิดขึ้นได้ในขั้นตอนดำเนินการ
2. บุคลากรของสำนักเทคโนโลยีดิจิทัลและสารสนเทศสามารถปฏิบัติงานแทนกันได้ในกรณีที่มีการปรับเปลี่ยนผู้ดูแลระบบ
3. บุคลากรของสำนักเทคโนโลยีดิจิทัลและสารสนเทศสามารถใช้คู่มือเป็นแนวทางในการปรับปรุงกระบวนการบริหารจัดการบัญชีให้มีประสิทธิภาพมากขึ้น

1.4 ขอบเขต

การจัดทำคู่มือฉบับนี้ มีขอบเขตอ้างอิงการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ได้แก่ การสร้าง การเปลี่ยนแปลง การยกเลิก การกำหนดสิทธิเบื้องต้นบัญชีผู้ใช้งาน ของกลุ่มผู้ใช้งานหลัก ได้แก่ นักศึกษา บุคลากร ศิษย์เก่า อีเมลกลางสำหรับหน่วยงานหรือหลักสูตร ของสถาบันบัณฑิตพัฒนบริหารศาสตร์ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System)

1.5 คำจำกัดความเบื้องต้น

1. สถาบัน หมายถึง สถาบันบัณฑิตพัฒนบริหารศาสตร์
2. สำนัก หมายถึง สำนักเทคโนโลยีดิจิทัลและสารสนเทศ
3. NetID หมายถึง บัญชีผู้ใช้งานระบบ Microsoft 365 ของสถาบัน
4. ระบบ AMS หมายถึง ระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน (Account Management System
5. ระบบ AD หมายถึง ระบบที่ทำหน้าที่จัดเก็บข้อมูลต่างๆ เช่น บัญชีผู้ใช้ (User) กลุ่ม (Group) รายชื่อทรัพยากร ของสถาบัน ไว้ด้วยกัน
6. ระบบ REG หมายถึง ระบบบริการการศึกษา
7. ระบบฐานข้อมูลบุคลากร หมายถึง ระบบ MIS
8. ระบบ MES หมายถึง ระบบติดตามและประเมินผลการปฏิบัติงาน

บทที่ 2
โครงสร้างการบริหารอัตรากำลัง บทบาทหน้าที่ความรับผิดชอบ

บทที่ 2 ของคู่มือปฏิบัติงาน เรื่อง การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน(Account Management System) จะกล่าวถึงประวัติความเป็นมา การบริหารงาน โครงสร้างและบทบาทหน้าที่ความรับผิดชอบของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และของส่วนงานโครงสร้างพื้นฐานและความมั่นคงปลอดภัย รวมไปถึงหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน โดยมีรายละเอียด ดังนี้

2.1 โครงสร้างการบริหารและอัตรากำลังของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2.2 ขอบข่ายภาระงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2.3 หน้าที่ความรับผิดชอบของส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย

2.4 หน้าที่ความรับผิดชอบของตำแหน่ง

2.5 ลักษณะงานที่ปฏิบัติงานของตำแหน่ง

2.1 โครงสร้างการบริหารและอัตรากำลังของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

ประวัติความเป็นมา และการบริหารของสำนักเทคโนโลยีดิจิทัลและสารสนเทศมีรายละเอียดกล่าวถึง ดังนี้

2.1.1 ประวัติความเป็นมา

2.1.2 โครงสร้างการบริหารงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2.1.3 โครงสร้างองค์กร และโครงสร้างอัตรากำลัง

2.2.1 ประวัติความเป็นมา

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ เดิมชื่อ “ศูนย์การศึกษาระบบสารสนเทศ” ได้ก่อตั้งขึ้นเมื่อวันที่ 27 กรกฎาคม พ.ศ.2527 และในปี พ.ศ. 2564 สถาบันได้มีประกาศสถาบันฯ เรื่อง การแบ่งหน่วยงานภายในส่วนงานของสถาบันบัณฑิตพัฒนบริหารศาสตร์ ลงวันที่ 17 ธันวาคม 2564 โดยสำนักได้รับการเปลี่ยนชื่อเป็น “สำนักเทคโนโลยีดิจิทัลและสารสนเทศ” ตั้งแต่วันที่ 1 มกราคม 2565

- **ปรัชญาและปณิธาน**

สำนักเทคโนโลยีสารสนเทศมีจุดมุ่งหมายในการให้บริการเทคโนโลยีสารสนเทศ เพื่อสนับสนุนสถาบันในการดำเนินการตามพันธกิจอย่างราบรื่น และมีประสิทธิภาพ

- **วิสัยทัศน์**

เป็นหน่วยงานให้บริการเทคโนโลยีสารสนเทศที่มีคุณภาพระดับสากล

- **พันธกิจ**

1. ให้บริการเทคโนโลยีสารสนเทศแก่อาจารย์ นักศึกษา และบุคลากรภายในสถาบัน เพื่อให้การดำเนินพันธกิจของสถาบันเป็นไปอย่างราบรื่น และมีประสิทธิภาพ
2. พัฒนาระบบสารสนเทศเพื่อสนับสนุนการดำเนินงานของสถาบันด้านการเรียนการสอน และการบริหารจัดการให้เหมาะสมและทันต่อการเปลี่ยนแปลงของสภาวการณ์
3. พัฒนาศักยภาพทางคอมพิวเตอร์ด้านความสามารถในการใช้คอมพิวเตอร์ และโปรแกรมใช้งานที่เกี่ยวข้องให้แก่นักศึกษาระดับปริญญาโท และปริญญาเอกของสถาบัน
4. จัดฝึกอบรมด้านคอมพิวเตอร์ และเทคโนโลยีสารสนเทศให้กับบุคลากรของสถาบัน ตั้งแต่ระดับผู้ใช้งานจนถึงระดับผู้บริหาร
5. ให้บริการวิชาการทางคอมพิวเตอร์ และเทคโนโลยีสารสนเทศแก่หน่วยงานภายนอก อาทิ การศึกษาวิเคราะห์ และจัดวางระบบงาน การวางแผนด้านระบบสารสนเทศ เป็นต้น
6. สนับสนุนพันธกิจด้านการทำนุบำรุงศิลปวัฒนธรรมของสถาบันในเชิงบูรณาการ

- **ค่านิยมร่วม**

1. Service-mindedness หมายถึง การบริการด้วยใจ
2. Smartness หมายถึง การปฏิบัติงานที่ถูกต้อง และมีความรู้จริง
3. Smoothness หมายถึง ความราบรื่น ไม่ติดขัดในการดำเนินงาน
4. Securement หมายถึง ความมั่นคงปลอดภัย
5. Speediness หมายถึง ความรวดเร็วทันต่อความต้องการใช้งาน

ที่มา : เว็บไซต์สำนักเทคโนโลยีดิจิทัลและสารสนเทศ (“วิสัยทัศน์ พันธกิจ,” 2568)

2.2.2 โครงสร้างการบริหารงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

สำนักเทคโนโลยีดิจิทัลและสารสนเทศมีโครงสร้างการบริหารงานภายในสำนัก ประกอบด้วย

1) คณะกรรมการประจำสำนัก ประกอบด้วย ผู้อำนวยการสำนัก เป็นประธานกรรมการ รองผู้อำนวยการสำนัก (ถ้ามี) คณาจารย์ประจำของสถาบัน เป็นกรรมการ และผู้อำนวยการกองบริหารงานสำนัก เป็นเลขานุการ โดยมีอำนาจหน้าที่ตามข้อ 16 ของข้อบังคับสถาบันบัณฑิตพัฒนบริหารศาสตร์ ว่าด้วยคุณสมบัติ หลักเกณฑ์ และวิธีการได้มาซึ่งคณะกรรมการประจำคณะ วิทยาลัย สำนัก และส่วนงานที่เรียกชื่ออย่างที่มีฐานะเทียบเท่าคณะ วิทยาลัยหรือสำนัก พ.ศ. 2562

2) คณะกรรมการกองทุนพัฒนาเทคโนโลยี ประกอบด้วย รองอธิการบดีที่อธิการบดีมอบหมาย เป็นประธาน ผู้บริหารหรือผู้แทนส่วนงานของสถาบันซึ่งอธิการบดีแต่งตั้งตามคำแนะนำของผู้อำนวยการสำนัก อย่างน้อย 3 คน แต่ไม่เกิน 7 คน เป็นกรมการ ผู้อำนวยการสำนัก เป็นกรรมการและเลขานุการ รองผู้อำนวยการสำนัก (ถ้ามี) เป็นกรรมการและผู้ช่วยเลขานุการ ผู้อำนวยการกองบริหารงานสำนัก เป็นผู้ช่วยเลขานุการ โดยมีอำนาจหน้าที่ตามข้อ 9 ของระเบียบสถาบันบัณฑิตพัฒนบริหารศาสตร์ ว่าด้วยการบริหารกองทุนพัฒนาเทคโนโลยี พ.ศ. 2566

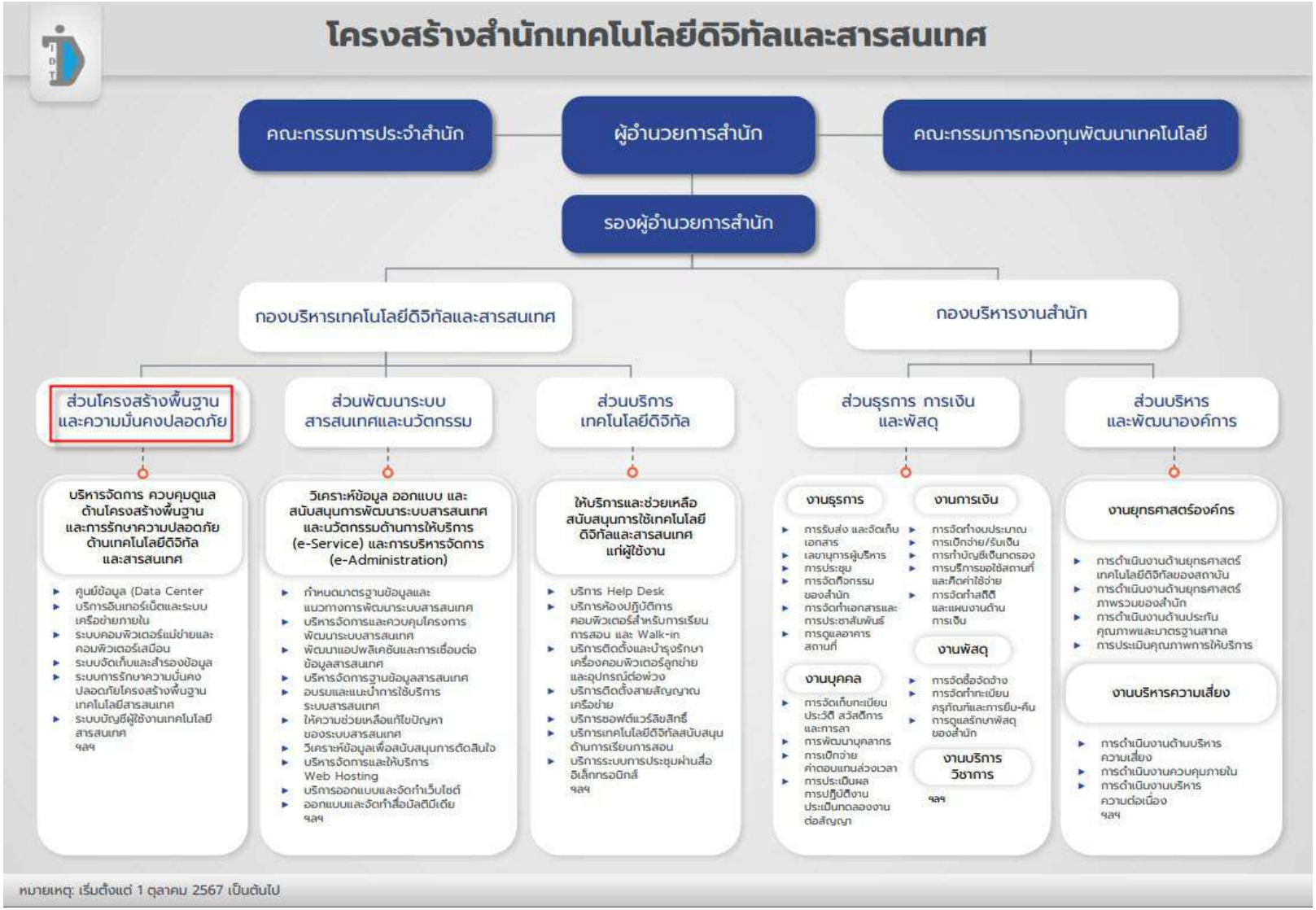
2.2.3 โครงสร้างองค์กร และโครงสร้างอัตรากำลัง

ปัจจุบันสำนักเทคโนโลยีดิจิทัลและสารสนเทศมีบุคลากรรวมทั้งสิ้น 31 คน แบ่งเป็นข้าราชการ จำนวน 2 คน พนักงานสถาบันสายวิชาการ จำนวน 1 คน พนักงานสถาบันสายสนับสนุนวิชาการ จำนวน 25 คน ลูกจ้างชั่วคราว จำนวน 3 คน ซึ่งสำนักจัดแบ่งโครงสร้างบริหารงานเป็น 2 กอง ดังนี้

- กองบริหารเทคโนโลยีดิจิทัลและสารสนเทศ มีบุคลากรจำนวน 21 คน
- กองบริหารงานสำนักเทคโนโลยีดิจิทัลและสารสนเทศ มีบุคลากรจำนวน 9 คน

โดยมีรายละเอียดตามแผนภูมิภาพที่ 2.1.3.1 การจัดแบ่งหน่วยงานสำนักเทคโนโลยีดิจิทัลและสารสนเทศ และแผนภูมิที่ 2.1.3.2 โครงสร้างอัตรากำลังของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

ภาพที่ 2-1 แสดงโครงสร้างของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ



ที่มา : สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ข้อมูล ณ วันที่ 1 ตลาคม 2567

ภาพที่ 2-2 : แสดงโครงสร้างอัตรากำลังสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

ที่มา : สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ข้อมูล ณ วันที่ 1 ตุลาคม 2567

2.2 ขอบข่ายภาระงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ เป็นหน่วยงานสนับสนุนของสถาบัน มีบทบาทหน้าที่รับผิดชอบในการบริหารจัดการด้านเทคโนโลยีดิจิทัลและระบบสารสนเทศของสถาบัน ดูแลด้านโครงสร้างพื้นฐานและความมั่นคงปลอดภัย ด้านพัฒนาและดูแลระบบสารสนเทศ และให้บริการเทคโนโลยีดิจิทัล โดยสำนักเทคโนโลยีดิจิทัลและสารสนเทศจัดแบ่งโครงสร้างออกเป็น 2 กอง ดังนี้

2.2.1 กองบริหารเทคโนโลยีดิจิทัลและสารสนเทศ

2.2.2 กองบริหารงานสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2.2.1 กองบริหารเทคโนโลยีดิจิทัลและสารสนเทศ

ดำเนินการด้านเกี่ยวกับเทคโนโลยีสารสนเทศของสถาบัน ทั้งด้านการให้บริการเครือข่าย การรักษาความมั่นคงปลอดภัยของเทคโนโลยีดิจิทัล และการดูแล พัฒนาและบำรุงรักษาระบบสารสนเทศและการให้บริการเทคโนโลยีดิจิทัล โดยแบ่งเป็น 3 ส่วน ดังนี้

- **ส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย** มีขอบเขตภาระงานในการบริหารจัดการควบคุมดูแลด้านโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีดิจิทัลและสารสนเทศ ประกอบด้วย ศูนย์ข้อมูล (Data Center) บริการอินเทอร์เน็ตและระบบเครือข่ายภายในระบบคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์แม่ข่ายเสมือน ระบบจัดเก็บและสำรองข้อมูล ระบบการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ระบบบัญชีผู้ใช้งานเทคโนโลยีสารสนเทศ ฯลฯ

- **ส่วนพัฒนาระบบสารสนเทศและนวัตกรรม** มีขอบเขตภาระงานในการวิเคราะห์ข้อมูลออกแบบและสนับสนุนการพัฒนาระสารสนเทศและนวัตกรรมด้านการให้บริการ (e-Service) และการบริหารจัดการ (e-Administration) ประกอบด้วย กำหนดมาตรฐานข้อมูลและแนวทางการพัฒนาระบบสารสนเทศ บริหารจัดการและควบคุมโครงการพัฒนาระบบสารสนเทศ พัฒนาแอปพลิเคชันและการเชื่อมต่อข้อมูลสารสนเทศ บริหารจัดการฐานข้อมูลสารสนเทศ อบรมและแนะนำการใช้บริการระบบสารสนเทศ ให้ความช่วยเหลือแก้ไขปัญหาของระบบสารสนเทศ วิเคราะห์ข้อมูลเพื่อสนับสนุนการตัดสินใจ บริหารจัดการและให้บริการ Web Hosting บริการออกแบบและจัดทำเว็บไซต์ ออกแบบและจัดทำสื่อมัลติมีเดียล ฯลฯ

- **ส่วนบริการเทคโนโลยีดิจิทัล** มีขอบเขตภาระงานให้บริการและช่วยเหลือสนับสนุน

การใช้เทคโนโลยีดิจิทัลและสารสนเทศแก่ผู้ใช้งาน ประกอบด้วย บริการ Help Desk บริการห้องปฏิบัติการคอมพิวเตอร์สำหรับการเรียนการสอน และ Walk-in บริการติดตั้งและบำรุงรักษาเครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์ต่อพ่วง บริการติดตั้งสายสัญญาณเครือข่าย บริการซอฟต์แวร์ลิขสิทธิ์ บริการเทคโนโลยีดิจิทัลสนับสนุนด้านการเรียนการสอน บริการระบบการประชุมผ่านสื่ออิเล็กทรอนิกส์ ฯลฯ

2.2.2 กองบริหารงานสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

ดำเนินการด้านการบริหารจัดการงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ โดยแบ่งเป็น 2 ส่วน ดังนี้

- **ส่วนธุรการ การเงินและพัสดุ** มีขอบเขตภาระงานในการบริหารงานทั่วไปของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ประกอบด้วย

1) งานธุรการ ได้แก่ การรับส่งและจัดเก็บเอกสาร เลขานุการผู้บริหาร การประชุม การจัดกิจกรรมของสำนัก การจัดทำเอกสารและการประชาสัมพันธ์ การดูแลอาคารสถานที่

2) งานบุคคล ได้แก่ การจัดเก็บทะเบียนประวัติ สวัสดิการและการลา การขออัตรากำลัง การเบิกจ่ายค่าตอบแทนล่วงเวลา การประเมินผลการปฏิบัติงาน ประเมินทดลองงาน ต่อสัญญา

3) งานการเงิน ได้แก่ การจัดทำงบประมาณ การเบิกจ่าย/รับเงิน การทำบัญชีเงินทดรอง การบริการขอใช้สถานที่และคิดค่าใช้จ่าย การจัดทำสถิติและแผนงานด้านการเงิน

4) งานพัสดุ ได้แก่ การจัดซื้อจัดจ้าง การจัดทำทะเบียนครุภัณฑ์และการยืม-คืน การดูแลรักษาพัสดุของสำนัก 5) งานบริการวิชาการ ได้แก่ การจัดอบรมให้แก่บุคลากรภายในสำนักและสถาบัน และการจัดอบรมให้แก่บุคคลภายนอก ฯลฯ

- **ส่วนบริหารและพัฒนาองค์การ** มีขอบเขตภาระงานในการจัดทำแผนงาน และแผนงบประมาณ รวมทั้งติดตาม รายงานและวิเคราะห์ผล บริหารจัดการและพัฒนาระบบการทำงานของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ประกอบด้วย 1) งานยุทธศาสตร์องค์กร ได้แก่ การดำเนินงานด้านยุทธศาสตร์เทคโนโลยีดิจิทัลของสถาบัน การดำเนินงานด้านยุทธศาสตร์ภาพรวมของสำนัก การดำเนินงานด้านประกันคุณภาพและมาตรฐานสากล การประเมินคุณภาพการให้บริการ 2) งานบริหารความเสี่ยง ได้แก่ การดำเนินงานด้านบริหารความเสี่ยง การดำเนินงานควบคุมภายใน การดำเนินงานบริหารความต่อเนื่อง ฯลฯ

2.3 หน้าที่ความรับผิดชอบของส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย

ส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย อยู่ภายใต้กองบริหารเทคโนโลยีดิจิทัลและสารสนเทศ มีบุคลากรภายในส่วนจำนวน 5 คน ซึ่งมีหน้าที่รับผิดชอบดังนี้

1) ศูนย์ข้อมูล (Data Center) ได้แก่ การบริหารจัดการควบคุมดูแลห้องเครือข่าย และคอมพิวเตอร์แม่ข่ายหลักที่ให้บริการของสถาบัน
2) บริการอินเทอร์เน็ตและระบบเครือข่ายภายใน ได้แก่ ดูแลและแก้ไขปัญหาระบบเครือข่ายภายในสถาบันให้สามารถใช้งานได้อย่างมีประสิทธิภาพ รวมทั้งดูแลระบบอินเทอร์เน็ตของสถาบันประสานงานกับผู้ให้บริการเมื่อเกิดปัญหา
3) ระบบคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์แม่ข่ายเสมือน ได้แก่ การสร้าง และบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย และคอมพิวเตอร์แม่ข่ายเสมือนเพื่อรองรับระบบสารสนเทศต่างๆของสถาบัน
4) ระบบจัดเก็บและสำรองข้อมูล ได้แก่ การสำรองและกู้คืนข้อมูลระบบสารสนเทศ และระบบ VPS ของสถาบัน
5) ระบบการรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ได้แก่ การบริหารจัดการไฟร์วอล ระบบป้องกันไวรัส ระบบควบคุมการเข้าถึงศูนย์ข้อมูล การปรับปรุงช่องโหว่ต่างๆของอุปกรณ์เครือข่าย และคอมพิวเตอร์แม่ข่าย
6) ระบบบัญชีผู้ใช้งานเทคโนโลยีสารสนเทศ ได้แก่ การให้บริการบัญชีผู้ใช้งานระบบสารสนเทศต่างๆของสถาบันแก่ บุคลากร นักศึกษา อาจารย์พิเศษ ผู้อบรม/สัมมนา และบัญชีผู้ใช้งานอื่นๆตามที่ได้รับมอบหมาย รวมทั้งการทบทวนบัญชีผู้ใช้งานให้เป็นปัจจุบัน

2.4 หน้าที่ความรับผิดชอบของตำแหน่ง

ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ ปฏิบัติงานในส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย สังกัดสำนักเทคโนโลยีดิจิทัลและสารสนเทศ มีหน้าที่และความรับผิดชอบในด้านต่างๆ ดังนี้

2.4.1 ด้านปฏิบัติการ

2.4.2 ด้านวางแผน

2.4.3 ด้านการประสานงาน

2.4.4 ด้านการบริการ

2.4.1 ด้านปฏิบัติการ

1) ศึกษา วิเคราะห์ และกำหนดคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย ระบบงานประยุกต์ จัดการระบบการทำงานของเครื่อง การติดตั้งระบบเครื่อง ทดสอบคุณสมบัติด้านเทคนิคของเครื่องและอุปกรณ์ เพื่อให้ได้อุปกรณ์คอมพิวเตอร์ที่เป็นมาตรฐานเดียวกันทั้งหน่วยงาน
2) ออกแบบระบบงาน ข้อมูล การประมวลผล การสื่อสาร ระบบข่ายงาน ชุดคำสั่งและฐานข้อมูลตามความต้องการของหน่วยงาน ติดตั้ง บำรุงรักษาเครื่องคอมพิวเตอร์ ระบบอุปกรณ์ต่าง ๆ ชุดคำสั่งระบบปฏิบัติการ เพื่อสนับสนุนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
3) ศึกษา ค้นคว้า ทดลอง วิเคราะห์ สังเคราะห์ หรือวิจัย จัดทำเอกสารวิชาการ คู่มือเกี่ยวกับงานในความรับผิดชอบ เผยแพร่ผลงานทางด้านวิทยากรคอมพิวเตอร์ ติดตามและพัฒนาเทคโนโลยี เพื่อกำหนดลักษณะและมาตรฐานในการปฏิบัติงาน หาวิธีในการแก้ไขปัญหาหรือพัฒนาแนวทางวิธีการในการปฏิบัติงานให้มีประสิทธิภาพยิ่งขึ้น
4) ให้บริการวิชาการด้านต่าง ๆ เช่น ช่วยสอน ฝึกอบรม เผยแพร่ความรู้ความเข้าใจเกี่ยวกับหลักการและวิธีการของงานด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา แนะนำ ตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ เข้าร่วมประชุมคณะกรรมการต่าง ๆ ที่ได้รับแต่งตั้ง เพื่อให้ข้อมูลทางวิชาการประกอบการพิจารณาและตัดสินใจและปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

2.4.2 ด้านวางแผน

ร่วมกำหนดนโยบายและแผนงานของส่วนงาน วางแผนหรือร่วมวางแผนการทำงานตามแผนงานหรือโครงการของสำนัก แก้ไขปัญหาในการปฏิบัติงาน เพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

2.4.3 ด้านการประสานงาน

1) ประสานการทำงานร่วมกันโดยให้ความเห็นและคำแนะนำเบื้องต้นแก่สมาชิกภายในสำนักหรือหน่วยงานอื่น เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้
2) ให้ข้อคิดเห็นหรือคำแนะนำเบื้องต้นแก่สมาชิกในทีมงาน หรือบุคคล หรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจและความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

2.4.4 ด้านการบริการ

1) ให้คำปรึกษา แนะนำ ฝึกอบรม ถ่ายทอดความรู้ ทางด้านวิทยากรคอมพิวเตอร์แก่ผู้รับบริการทั้งภายในและภายนอกหน่วยงาน รวมทั้งตอบปัญหาและชี้แจงเรื่องต่าง ๆ เกี่ยวกับงานในหน้าที่ เพื่อให้มีความรู้ความเข้าใจ และสามารถดำเนินงานได้อย่างถูกต้อง
2) พัฒนาข้อมูล จัดทำเอกสารวิชาการ สื่อเอกสารเผยแพร่ ให้บริการวิชาการด้านวิทยาการคอมพิวเตอร์ที่ซับซ้อน เพื่อก่อให้เกิดการแลกเปลี่ยนเรียนรู้ที่สอดคล้องและสนับสนุนภารกิจของสำนัก

2.5 ลักษณะงานที่ปฏิบัติของตำแหน่ง

ตำแหน่งนักวิชาการคอมพิวเตอร์ปฏิบัติการ ปฏิบัติงานส่วนโครงสร้างพื้นฐานและความมั่นคงปลอดภัย สังกัดสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ปฏิบัติงานในด้านต่างๆ โดยมีรายละเอียด ดังนี้

2.5.1 ด้านปฏิบัติการ
2.5.2 ด้านวางแผน
2.5.3 ด้านการประสานงาน
2.5.4 ด้านการบริการ
2.5.5 ด้านอื่นๆ

2.5.1 ด้านปฏิบัติการ

1) การบริหารจัดการบัญชีผู้ใช้งานประเภทต่างๆ ให้มีความถูกต้องตามประเภทของกลุ่มผู้ใช้งาน
2) บริหารจัดการสิทธิของผู้ใช้งาน เพื่อให้ผู้ใช้งานได้สิทธิตามประเภทของผู้ใช้งานแต่ละกลุ่ม การควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงระบบเครือข่าย หรือ Microsoft 365
3) ทบทวนสิทธิบัญชีผู้ใช้งาน เพื่อให้ข้อมูลเป็นปัจจุบัน ป้องกันการเข้าถึงระบบเครือข่ายของสถาบัน หรือ Microsoft 365 จากผู้ไม่มีสิทธิ์ในการใช้งาน
4) บริหารจัดการและดูแล ระบบ ICS Sharepoint ของสถาบันบน Microsoft 365
5) บริหารจัดการระบบการเข้าถึงพื้นที่ โดยดูแลเครื่องสแกนลายนิ้วมือและสแกนบัตรของสำนัก เพื่อให้เกิดความปลอดภัยต่อบุคลากร ทรัพย์สินของหน่วยงาน

6) งานดูแลศูนย์ข้อมูลหลัก (Data Center) ที่อยู่ในความรับผิดชอบของกลุ่มงาน เพื่อไม่ให้เกิดความเสียหายต่อระบบโครงสร้างพื้นฐานหลักของสถาบัน
7) การบริหารจัดการระบบป้องกันไวรัส (Antivirus) ที่ให้บริการกับผู้ใช้งานของสถาบัน
8) ควบคุมและดูแลครุภัณฑ์เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย
9) ทำการจัดซื้อ หรือตรวจรับระบบสารสนเทศ ซอฟต์แวร์ หรืออุปกรณ์ต่างๆ ที่จัดหาในโครงการภายใต้ความรับผิดชอบของส่วนงาน หรือหน่วยงานอื่นๆ ที่ขอความร่วมมือ
10) ปฏิบัติงานและสนับสนุนงานอื่นๆ ตามที่ได้รับมอบหมาย เพื่อสนับสนุนให้สถาบันบรรลุภารกิจที่กำหนดไว้

2.5.2 ด้านวางแผน

1) จัดทำแผนการปฏิบัติงานตามที่ได้รับมอบหมายและปฏิบัติงานตามแผนที่กำหนด
2) จัดทำแผนและติดตามผล การบำรุงรักษาอุปกรณ์ทางด้านโครงสร้างพื้นฐานทั้งหมด
3) จัดทำแผนเพื่อสนับสนุนการรับรองมาตรฐาน ISO 27001 ได้แก่ แผนการติดตามการเปลี่ยนแปลงใน Event-Incident Log แผนการทบทวน Access Rights Matrix

2.5.3 ด้านการประสานงาน

1) ประสานงานกับหน่วยงานต่างๆ ภายในสถาบัน เพื่อให้การบริหารจัดการบัญชีถูกต้อง และรวดเร็ว
2) ประสานงานกับบริษัทผู้รับจ้างเพื่อพัฒนา ปรับปรุงหรือแก้ไขระบบสารสนเทศ บำรุงรักษาระบบโครงสร้างพื้นฐาน ให้ใช้งานได้อย่างถูกต้อง และมีประสิทธิภาพ

2.5.4 ด้านการบริการ

1) ให้คำแนะนำวิธีการ และรายละเอียดการใช้งานบัญชี (Account) สำหรับบริการด้านต่างๆ
2) ติดตั้งโปรแกรมป้องกันไวรัส และแก้ไขปัญหาที่อาจเกิดจากการถูกโจมตีด้วยไวรัสคอมพิวเตอร์ หรือโปรแกรมที่ไม่พึงประสงค์
3) ตอบคำถามข้อสงสัย และช่วยแก้ไขปัญหาที่เกิดขึ้นกับการใช้งานระบบ Microsoft 365 WiFi VPN รวมถึงให้คำแนะนำที่ถูกต้องเหมาะสม แก่ผู้ใช้งาน

2.5.5 ด้านอื่นๆ

4) ร่วมเป็นกรรมการต่าง ๆ ของสถาบันและของสานัก ตามที่ได้รับมอบหมาย

5) เป็นคณะทำงานด้านการประชาสัมพันธ์ของสำนัก

6) ศึกษาหาความรู้เพิ่มเติมเพื่อนำมาในการใช้พัฒนากระบวนการทำงานให้ดีขึ้น

บทที่ 3
หลักเกณฑ์ วิธีการปฏิบัติ และเงื่อนไข

Microsoft 365 เป็นบริการที่รวมแอพลิเคชันต่างๆ ของ Microsoft เช่น Microsoft Teams, Sharepoint, Outlook, OneDrive และอื่นๆ ซึ่งปัจจุบันสถาบันได้ใช้บริการของ Microsoft 365 เป็นบริการหลักในการเรียนการสอน ผู้ที่ได้รับมอบหมายให้ปฏิบัติงานบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ต้องคำนึงถึงความถูกต้อง รวดเร็ว และสิทธิที่ได้รับในการใช้งาน เนื่องจากบัญชีผู้ใช้งานระบบ Microsoft 365 นั้น สามารถใช้ในการล็อกอินเพื่อเข้าใช้งานระบบสารสนเทศต่างๆของสถาบันด้วย จึงมีความจำเป็นต้องมีความรู้ ความเข้าใจในเรื่องต่างๆ ดังนี้

3.1. หลักเกณฑ์การปฏิบัติงาน/ มาตรฐานการปฏิบัติงาน

3.2. วิธีการปฏิบัติงาน

3.3. เงื่อนไข ข้อสังเกต ข้อควรระวัง สิ่งที่ควรคำนึงในการปฏิบัติงาน

3.4. แนวคิด/ งานวิจัยที่เกี่ยวข้อง

3.5. วิธีการทำให้ผู้รับบริการมีความพึงพอใจ และวิธีประเมินผลการปฏิบัติงาน

3.6. จรรยาบรรณ/ คุณธรรม/ จริยธรรมในการปฏิบัติงาน

3.1 หลักเกณฑ์การปฏิบัติงาน/ มาตรฐานการปฏิบัติงาน

เพื่อให้การบริหารจัดการบัญชี Microsoft 365 เป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ มีความมั่นคงปลอดภัยด้านสารสนเทศ จำเป็นต้องมีการศึกษาและทำความเข้าใจในประกาศ ข้อกำหนดในการให้บริการดังนี้

3.1.1) การจัดบริการ Microsoft 365

3.1.2) นโยบายและแนวปฏิบัติในการรักษาคามมั่นคงปลอดภัยด้านสารสนเทศของสถาบันบัณฑิตพัฒนบริหารศาสตร์

3.1.3) ข้อมูลข่าวสารของราชการ

3.1.4) การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3.1.1 การจัดบริการ Microsoft 365

ผู้ปฏิบัติงานจำเป็นต้องรู้ และปฏิบัติตามประกาศสถาบัน เรื่องการจัดบริการ Microsoft 365 เพื่อให้การปฏิบัติงานเป็นไปด้วยความเรียบร้อย ถูกต้องตามข้อกำหนดของสถาบัน

3.1.1.1 ผู้มีสิทธิการใช้งาน Microsoft 365

1. นักศึกษาของสถาบัน
2. ผู้ปฏิบัติงานในสายวิชาการ
3. ผู้ปฏิบัติงานในสถาบันสายสนับสนุนวิชาการ
4. อาจารย์พิเศษและผู้ทรงคุณวุฒิภายนอก
5. ส่วนงานหรือหน่วยงานภายในสถาบัน

1. นักศึกษาของสถาบันมีสิทธิใช้งาน Microsoft 365 ดังนี้
   (1) นักศึกษาที่กำลังศึกษาอยู่ และที่สำเร็จการศึกษาแล้วเป็นระยะเวลาไม่เกิน ๙๐ วัน มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๓๐ GB และมีสิทธิการติดตั้งใช้งานโปรแกรม Microsoft Office บนเครื่องคอมพิวเตอร์ อุปกรณ์แท็บเล็ต และอุปกรณ์โทรศัพท์พกพา
   (2) นักศึกษาที่สำเร็จการศึกษาแล้วเป็นระยะเวลาตั้งแต่ ๙๐ วันขึ้นไป มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๓๐ GB เท่านั้น และสถาบันจะระงับสิทธิการใช้งานหลังจานักศึกาสำเร็จการศึกษาแล้วเป็นระยะเวลาตั้งแต่ ๒ ขึ้นไป
   (3) นักศึกษาที่สิ้นสภาพการเป็นนักศึกษาแต่ไม่สำเร็จการศึกษา สถาบันจะระงับสิทธิการใช้งานตั้งแต่วันที่สิ้นสภาพการเป็นนักศึกษา
2. ผู้ปฏิบัติงานในสถาบันสายวิชาการมีสิทธิใช้งาน Microsoft 365 ดังนี้
   (1) ผู้ปฏิบัติงานในสถาบันสายวิชาการ มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๑๐๐ GB และมีสิทธิการติดตั้งใช้งานโปรแกรม Microsoft Office บนเครื่องคอมพิวเตอร์ อุปกรณ์แท็บเล็ต และอุปกรณ์โทรศัพท์พกพา
   (2) ผู้ปฏิบัติงานในสถาบันสายวิชาการที่เกษียณอายุงานมีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๑๐๐ GB เท่านั้น

(3) ผู้ปฏิบัติงานในสถาบันสายวิชาการที่พ้นสภาพการเป็นผู้ปฏิบัติงานในสถาบันโดยมิใช่เหตุเกษียณอายุงาน สถาบันจะระงับสิทธิการใช้งานตั้งแต่วันที่พ้นสภาพการเป็นผู้ปฏิบัติงานในสถาบัน

ผู้ปฏิบัติงานในสถาบันสายวิชาการที่พ้นสภาพจากการเป็นผู้ปฏิบัติงานในสถาบันด้วยเหตุการลาออก และมีความจำเป็นต้องใช้ Microsoft 365 ต่อไป สามารถแจ้งความประสงค์ขอต่ออายุการใช้งานพร้อมเหตุผลความจำเป็นผ่านส่วนงานต้นสังกัดก่อนลาออก ไปยังสำนักเทคโนโลยีดิจิทัลและสารสนเทศเพื่อขอต่ออายุสิทธิการใช้งานเป็นระยะเวลาได้ไม่เกิน ๑ ปี โดยจะมีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive ไม่เกิน ๑๐๐ GB เท่านั้น และสามารถขอต่ออายุการใช้งานเพิ่มได้อีกไม่เกิน ๑ ปี เมื่อครบกำหนดระยะเวลาต่ออายุการใช้งานอล้ว สถาบันจะระงับสิทธิการใช้งาน

3. ผู้ปฏิบัติงานในสถาบันสายสนับสนุนวิชาการมีสิทธิใช้งาน Microsoft 365 ดังนี้

(1) ผู้ปฏิบัติงานในสถาบันสายสนับสนุนวิชาการ มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๕๐ GB และมีสิทธิการติดตั้งการใช้งานโปรแกรม Microsoft Office บนเครื่องคอมพิวเตอร์ อุปกรณ์แท็บเล็ต และอุปกรณ์โทรศัพท์พกพา

(2) ผู้ปฏิบัติงานในสถาบันสายสนับสนุนวิชาการที่เกษียณอายุงาน มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๕๐ GB เท่านั้น และสถาบันจะระงับสิทธิการใช้งานหลังจากเกษียณอายงานแล้วเป็นระยะเวลาตั้งแต่ ๒ ปีขึ้นไป

(3) ผู้ปฏิบัติงานสายสนับสนุนวิชาการ ที่พ้นสภาพการเป็นผู้ปฏิบัติงานในสถาบันโดยไม่ใช่เหตุเกษียณอายุงาน สถาบันจะระงับสิทธิการใช้งานตั้งแต่วันที่พ้นสภาพการเป็นผู้ปฏิบัติงานในสถาบัน

ผู้ปฏิบัติงานในสถาบันสายสนับสนุนวิชาการที่พ้นสภาพจากการเป็นผู้ปฏิบัติงานในสถาบันด้วยเหตุการลาออก และมีความจำเป็นต้องใช้ Microsoft 365 ต่อไป สามารถแจ้งความประสงค์ขอต่ออายุการใช้งานพร้อมเหตุผลความจำเป็นผ่านส่วนงานต้นสังกัดก่อนลาออก ไปยังสำนักเทคโนโลยีดิจิทัลและสารสนเทศเพื่อขอต่ออายุสิทธิการใช้งานเป็นระยะเวลาได้ไม่เกิน ๑ ปี โดยจะมีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive ไม่เกิน ๕๐ GB เท่านั้น และสามารถขอต่ออายุการใช้งานเพิ่มได้อีกไม่เกิน ๑ ปี เมื่อครบกำหนดระยะเวลาต่ออายุการใช้งานอล้ว สถาบันจะระงับสิทธิการใช้งาน

4. อาจารย์พิเศษและผู้ทรงคุณวุฒิภายนอกมีสิทธิใช้งาน Microsoft 365 แบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๑๐ GB

สถาบันจะระงับสิทธิการใช้งานของอาจารย์พิเศษและผู้ทรงคุณวุฒิภายนอก หากส่วนงานหรือหน่วยงานภายในที่ขอรับบริการไม่ได้แจ้งยืนยันการใช้บริการต่อเนื่อง เมื่อมีการทบทวนการใช้บริการ Microsoft 365 ประจำปี หรือเมื่อครบกำหนดระยะเวลาที่ขอรับบริการ

5. บัญชีส่วนงานหรือหน่วยงานภายใน มีสิทธิใช้งานแบบออนไลน์ พร้อมพื้นที่จัดเก็บข้อมูล OneDrive จำนวนไม่เกิน ๔๐ GB

3.1.1.2 การกำหนดสิทธิ การระงับสิทธิ การยกเลิกสิทธิการใช้งานบัญชี Microsoft 365

1. ให้สำนักเทคโนโลยีดิจิทัลและสารสนเทศดำเนินการกำหนดสิทธิการใช้งานและพื้นที่จัดเก็บข้อมูลใน Microsoft SharePoint และ Microsoft Teams ในระบบ Microsoft 365 ของสถาบัน
2. นอกจากการระงับสิทธิการใช้งานตามที่กำหนดไว้ในข้อ 1) ถึงข้อ 4) สถาบันอาจระงับสิทธิการใช้งานของผู้มีสิทธิการใช้งาน ในกรณีดังต่อไปนี้
   (1) สถาบันตรวจพบว่ามีการใช้งานที่ผิดปกติและอาจนำไปสู่การกระทำความผิดต่อกฎหมาย หรือขัดต่อกฎระเบียบ ข้อบังคับ และนโยบายของถสถาบัน รวมถึงข้อตกลงการใช้บริการของ Microsoft
   (2) สถาบันตรวจพบว่ามีการใช้งานที่อาจไม่เหมาะสม ขัดต่อศีลธรรม หรือละเมิดสิทธิ์ของผู้อื่นทางใดทางหนึ่ง
3. สถาบันจะทำการลบข้อมูลของผู้มีสิทธิใช้งานระบบ Microsoft 365 เมื่อสิทธิการใช้งานสิ้นสุดลง และสถาบันจะไม่รับผิดชอบต่อผู้มีสิทธิใช้งานหรือบุคคลอื่นใดสำหรับความเสียหาย หรือการสูญหาย ของข้อมูลใด ๆ ที่เกิดขึ้นอันเนื่องจากสิทธิการใช้งานสิ้นสุดลง
4. ให้ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลและสารสนเทศเป็นผู้พิจารณาอนุมัติให้ดำเนินการกำหนดและให้สิทธิการใช้งาน การระงับสิทธิการใช้งาน และการยกเลิกสิทธิการใช้งานนอกเหนือจากที่กำหนดในประกาศนี้

3.1.1.3 หน้าที่ของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

1. บริหารจัดการและควบคุมการใช้งาน Microsoft 365 ให้เป็นไปตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365
2. ทบทวนสิทธิการใช้งาน Microsoft 365 อย่างน้อยปีละ 1 ครั้ง

3.1.2 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันบัณฑิตพัฒนบริหารศาสตร์

ตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. ๒๕๖๔ ผู้ปฏิบัติงานจำเป็นต้องรู้ และทำความเข้าใจ ในหลักเณฑ์การปฏิบัติงาน มาตรฐานการปฏิบัติงาน เอกสารแนบท้ายประกาศ ข้อ 3, 4 และภาคผนวก ข้อ 2, 3, 4, 7 ดังนี้

3.1.2.1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบัน โดยกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ดังนี้

1 การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ
ต้องดำเนินการตามข้อปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในภาคผนวก

2 การแบ่งกลุ่มบัญชีผู้ใช้
เพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศโดยระบุชื่อบัญชีผู้ใช้งานแยกกันแบบรายบุคคล ไม่ซ้ำซ้อนกัน ดังนี้

(2.1) นักศึกษา

(2.2) บุคลากร

(2.3) อาจารย์พิเศษ นักวิจัย กรรมการ ที่ปรึกษา

(2.4) บุคคลภายนอกที่เข้าอบรมหรือสัมมนา

(2.5) บุคคลอื่น ๆ ที่สถาบันมอบสิทธิให้

3 การลงทะเบียนผู้ใช้งาน (User Registration)

ต้องดำเนินการตามข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน ในภาคผนวก

4 การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

ต้องดำเนินการตามข้อปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน ในภาคผนวก โดยมีรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(4.1) ผู้ใช้งานที่มีชื่ออยู่ในบัญชีรายชื่อผู้ใช้งานมีสิทธิทั่วไปในการเข้าถึงระบบสารสนเทศพื้นฐาน ตามกลุ่มผู้ใช้งาน

(4.2) ให้หน่วยงานเจ้าของระบบเป็นผู้กำหนดสิทธิจำเพาะหรือสิทธิพิเศษรวมถึงกำหนดระยะเวลาในการใช้งาน

(4.3) การแจ้งขอใช้สิทธิ/เปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร

1 ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

2 ส่งถึงผู้บริหารของหน่วยงานเจ้าของระบบ

3 เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

4 หน่วยงานเจ้าของระบบส่งเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

(4.4) การให้สิทธิพิเศษกับผู้ใช้งาน ต้องได้รับความเห็นชอบจากอธิการบดีหรือผู้ที่ได้รับมอบหมายจากอธิการบดี

(4.5) การแจ้งยกเลิกสิทธิการใช้งานระบบสารสนเทศ

1 ผู้บริหารของหน่วยงานที่ขอใช้แจ้งยกเลิกสิทธิของผู้ใช้

2 ผู้ดูแลระบบทำการยกเลิกสิทธิในการใช้งานระบบตามคำขอและลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

(4.6) ผู้ดูแลระบบต้องทำการเพิกถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน หรือพ้นสภาพการเป็นนักศึกษาหรือบุคลากร หรือเมื่อผู้ใช้งานสิ้นสุดสภาพการใช้งาน

5 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(5.1) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ เข้าด้วยกัน

(5.2) ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นทราบ

(5.3) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(5.4) ผู้ดูแลระบบต้องกำหนดการใช้งานบัญชีผู้ใช้งานและรหัสผ่านกำหนดรหัสผ่านเริ่มต้นแยกเป็นรายบุคคล ให้กับผู้ใช้ให้ยากต่อการเดา เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

(5.5) ผู้ดูแลระบบต้องส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานภายในสถาบันด้วยวิธีการที่ปลอดภัย และผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานระบบงานครั้งแรก

(5.6) เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่าน ผู้ใช้งานต้องทำความเข้าใจและยอมรับสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(5.7) ผู้ใช้งานต้องทำการยืนยันตัวตน ที่ถูกต้อง ก่อนเปลี่ยนรหัสผ่าน

(5.8) ข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ หรือเครื่องหมายอื่นที่ทำให้ข้อมูลเป็นความลับ

(5.9) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

6 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบหรือเจ้าของระบบต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ และทบทวนสิทธิของผู้ใช้งานที่มีการเปลี่ยนแปลงสถานภาพ ได้แก่ การเปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน ดังนี้

(6.1) สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนทุกครั้งที่มีการปรับเปลี่ยนสถานะ ได้แก่ การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง

(6.2) สิทธิการเข้าถึงข้อมูลต้องได้รับการทบทวนและจัดสรรใหม่เมื่อมีการโยกย้ายบุคลากรระหว่างหน่วยงาน

(6.3) สิทธิการเข้าถึงพิเศษต้องได้รับการพิจารณาทบทวนตามระยะเวลาที่ได้รับอนุมัติการใช้งานและหรือทุกครั้งที่มีการปรับเปลี่ยนสิทธิการใช้งาน เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(6.4) ต้องมีการทบทวนอย่างน้อย ปีละ ๑ ครั้ง

1 ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานที่ได้รับสิทธิทั่วไปและผู้ใช้งานที่ได้รับสิทธิพิเศษ อย่างน้อยปีละ ๑ ครั้ง

2 ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานที่มีสิทธิระดับผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้ง

3 สิทธิการเข้าถึงการใช้งานสำหรับผู้ใช้งาน หมดอายุเมื่อผู้ใช้งานพ้นสภาพหรือผู้ใช้งานที่ได้รับสิทธิพิเศษไม่มีการใช้งานติดต่อกันเกิน ๑ปี

(6.5) บันทึกการเปลี่ยนแปลงสิทธิของผู้ใช้งานทุกครั้ง เพื่อใช้ในการทบทวนสิทธิการเข้าถึงผู้ใช้งานประจำปี

3.1.2.2 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

1 การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ผู้ใช้งานปฏิบัติตามข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ ในภาคผนวก

2 การระงับบัญชีจดหมายอิเล็กทรอนิกส์

(2.1) บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่สถาบันเอื้ออำนวยให้ผู้ใช้ ซึ่งผู้ใช้ไม่สามารถโอนสิทธิให้แก่ผู้อื่นใช้ได้ สถาบันคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิให้แก่ผู้ใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัยหรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์

(2.2) เมื่อผู้ใช้พ้นสภาพการเป็นบุคลากรของสถาบัน บัญชีจดหมายอิเล็กทรอนิกส์นั้นจะถูกระงับไป

(2.3) ผู้ใช้ที่พ้นสภาพการเป็นบุคลากรของสถาบัน สามารถร้องขอการขยายสิทธิการใช้บัญชีผู้ใช้เพื่อคงสิทธิการใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัดพร้อมแนบเหตุผลความจำเป็นส่งถึงสำนักเทคโนโลยีสารสนเทศ

การอนุญาตและระยะเวลาการขยายสิทธิให้เป็นอำนาจของผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

(2.4) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้บริหารของหน่วยงาน หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

(2.5) บัญชีของผู้ใช้จดหมายอิเล็กทรอนิกส์ สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบหากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบต่อการให้บริการระบบเครือข่ายมีประสิทธิภาพด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้ สำนักเทคโนโลยีสารสนเทศมีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

3.1.2.3 ข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน

1 จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศให้ผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน โดยสำนักเทคโนโลยีสารสนเทศหรือเจ้าของระบบเป็นผู้จัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

2 จัดทำเอกสารแสดงถึงสิทธิความรับผิดชอบของผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานซึ่งต้องลงนามรับทราบ

3 ในกรณีผู้ใช้งานต้องการระบุชื่อบัญชีผู้ใช้งานแบบกลุ่มภายใต้หน่วยงานเดียวกันที่มีบัญชีรายชื่อเดียวกัน ให้ผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานระบุรายชื่อผู้ใช้และผู้ที่รับผิดชอบในการดูแลบัญชีผู้ใช้ และแจ้งเป็นลายลักษณ์อักษรถึงสำนักเทคโนโลยีสารสนเทศ

4 ตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิจากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศ และบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิจากผู้บริหารอย่างชัดเจน

5 ตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

6 กำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

7 เมื่อมีการเปลี่ยนแปลงบัญชีผู้ใช้งานหรือผู้รับผิดชอบในการดูแลบัญชีผู้ใช้งานจะต้องเป็นลายลักษณ์อักษรถึงสำนักเทคโนโลยีสารสนเทศ

8 ตรวจสอบและมอบหมายสิทธิ หลักเกณฑ์ในการอนุญาตหรือการเพิกถอนสิทธิให้เข้าถึงระบบสารสนเทศ ต้องเป็นไปตามแนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้

3.1.2.4 ข้อปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน

1 ตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิอนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ
2 ตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน
3 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารแก่ผู้ใช้โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
4 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิพิเศษที่ได้รับด้วยว่าการเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ
5 ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด
6 การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ ผู้บริหารหน่วยงานของผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ
7 ผู้ดูแลระบบยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์มและลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด
8 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะที่เกี่ยวกับการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร
9 มีการทบทวนสิทธิการใช้งานอย่างน้อยปีละ ๑ ครั้ง

3.1.2.5 ข้อปฏิบัติการใช้งานรหัสผ่าน

1 เลือกรหัสผ่านที่ปลอดภัยและเก็บรักษารหัสผ่านไว้เป็นความลับอยู่ตลอดเวลา
2 ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ
3 ไม่ลักลอบใช้รหัสผ่าน หรือถอดรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น
4 รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที
5 ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น
6 กำหนดให้รหัสผ่านมีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ เข้าด้วยกัน
7 หลีกเลี่ยงการกำหนดรหัสผ่านจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม
8 หลีกเลี่ยงการใช้ตัวอักษรเรียงกัน ได้แก่ abcd 1234 และเลี่ยงการใช้ตัวอักษรซ้ำกัน ได้แก่ aaaa 8888
9 หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน และเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานอื่น ๆ ยกเว้นระบบที่มีการใช้ Single Sign-on หรือมีการยืนยันตัวบุคคลผ่านระบบบริหารจัดการบัญชีผู้ใช้งาน
10 หลีกเลี่ยงการจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
11 หลีกเลี่ยงการกำหนดให้เครื่องคอมพิวเตอร์จดจำรหัสผ่านของตนเองไว้
12 ควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือ มีผู้อื่นล่วงรู้
13 ควรเปลี่ยนรหัสผ่านหลังจากที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากการทำงาน
14 ควรเปลี่ยนรหัสผ่านทุกรอบระยะเวลา ๖ เดือน
15 ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

3.1.2.6 ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดี แห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของสถาบัน

2 ห้ามผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย ได้แก่ การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

3 ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว สถาบันไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

4 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

5 ผู้ใช้งานได้รับบัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

6 ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

7 ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

8 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาหรือสำนักเทคโนโลยีสารสนเทศ

3.1.3 ข้อมูลข่าวสารของราชการ

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 รองรับการคุ้มครองสิทธิรับรู้ข้อมูลหรือข่าวสาธารณะที่อยู่ในความครอบครองของหน่วยราชการ หน่วยงานของรัฐ รัฐวิสาหกิจและราชการส่วนท้องถิ่น ประชาชนมีโอกาสรู้ถึงสิทธิและหน้าที่ของตนอย่างเต็มที่ส่งเสริมให้การบริหารงานของรัฐเป็นไปอย่างโปร่งใส

3.1.3.1) ตามมาตรา 23

หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

(1) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(2) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3) จัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งเจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลปกติ

3.1.3.2) ตามมาตรา 24

หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงสนรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา ๒๖ วรรคหนึ่งเพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐ เพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (๓) (๔) (๕) (๖) (๗) (๘) และ (๙) ให้มีการจัดทำบัญชีแสดงเอกสารการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกระทรวง

3.1.3.3) ตามมาตรา ๒๕

ภายใต้บังคับมาตรา ๑๔ และมาตรา ๑๕ บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา ๙ วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายได้

ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอ ให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวันนับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ต่อคณะกรรมการ และไม่ว่ากรณีใดๆให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา ๒๓ มาตรา ๒๔ และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ หรือเจ้าของข้อมูลที่ถึงแก่กรรมแล้วก็ได้

<u>หมายเหตุ :</u> เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ ในระบบประชาธิปไตย การให้ประชาชนมีโอกาสกว้างขวางในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐเป็นสิ่งจำเป็น เพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความเป็นจริง อันเป็นการส่งเสริมให้มีความเป็นรัฐบาลโดยประชาชนมากยิ่งขึ้น สมควรกำหนดให้ประชาชนมีสิทธิได้รู้ข้อมูลข่าวสารของราชการ โดยมีข้อยกเว้นอันไม่ต้องเปิดเผยที่แจ้งชัดและจำกัดเฉพาะข้อมูลข่าวสารที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้เพื่อพัฒนาระบบประชาธิปไตยให้มั่นคงและจะยังผลให้ประชาชนมีโอกาสรู้ถึงสิทธิหน้าที่ของตนอย่างเต็มที่ เพื่อที่จะปกปักรักษาประโยชน์ของตนได้อีกประการหนึ่งด้วย ประกอบกับ

สมควรคุ้มครองสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อมกัน จึงจำเป็นต้องตราพระราชบัญญัตินี้

3.1.4 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ผู้ปฏิบัติงานพึงตระหนักถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ดังนี้

3.1.4.1 ตามมาตรา ๕

ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

3.1.4.2 ตามมาตรา ๖

ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

3.1.4.3 ตามมาตรา ๗

ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

3.1.4.4 ตามมาตรา ๘

ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

3.1.4.5 ตามมาตรา ๙

ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไมวาทั้งหมดหรือบางสวน ซึ่งข อมูลคอมพิวเตอรของผู้อื่นโดยมิชอบ ต่องระวางโทษจำคุกไมเกินห่าป หรือปรับไมเกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

3.1.4.6 ตามมาตรา ๑๐

ผู้ใดกระทำด่วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอรของผู้อื่นถูก ระงับ ชะลอ ขัดขวาง หรือรบกวนจนไมสามารถทำงานตามปกติได่ต่องระวางโทษจำคุกไมเกินห่าป หรือปรับไมเกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

3.1.4.7 ตามมาตรา ๑๑

ผู้ใดสงข่อมูลคอมพิวเตอรหรือจดหมายอิเล็กทรอนิกสแกบุคคลอื่นโดยปกปดหรือปลอมแปลง แหลงที่มาของการสงขอมูลดังกลาว อันเปนการรบกวนการใชระบบคอมพิวเตอรของ บุคคลอื่นโดยปกติสุข ตองระวางโทษปรับไมเกินหนึ่งแสนบาท

3.1.4.8 ตามมาตรา ๑๒

ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการ กระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของ ประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอัน เป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่ง แสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาท ถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หก หมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

ตามมาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตราย

แก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

3.1.4.9 ตามมาตรา ๑๓

ผู้ใดจำหนายหรือเผยแพรชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใชเปนเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ตองระวางโทษจำคุกไมเกินหนึ่งป หรือปรับไมเกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑

ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว

3.1.4.10 ตามมาตรา ๑๔

ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

3.1.4.11 ตามมาตรา ๑๕

ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ

3.1.4.12 ตามมาตรา ๑๖

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอายผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี

3.2 วิธีการปฏิบัติงาน

ตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365 สำนักเทคโนโลยีดิจิทัลและสารสนเทศ มีหน้าที่ดังนี้

3.2.1 บริหารจัดการและควบคุมการใช้งาน Microsoft 365 ให้เป็นไปตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

3.2.2 ทบทวนสิทธิการใช้งาน Microsoft 365 อย่างน้อยปีละ 1 ครั้ง

3.2.1 บริหารจัดการและควบคุมการใช้งาน Microsoft 365 ให้เป็นไปตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

NetID คือ บัญชีผู้ใช้งานเพื่อเข้าใช้งานบริการเทคโนโลยีสารสนเทศของสถาบันบัณฑิตพัฒนบริหารศาสตร์ ปัจจุบัน NetID มี 5 ประเภท ได้แก่

3.2.1.1 NetID สำหรับนักศึกษา

3.2.1.2 NetID สำหรับบุคลากร

3.2.1.3 NetID สำหรับอาจารย์พิเศษ

3.2.1.4 NetID สำหรับหน่วยงาน

3.2.1.5 NetID สำหรับ บุคคลภายนอกที่ใช้งานอินเทอร์เน็ตแบบชั่วคราว

3.2.1.1 NetID นักศึกษา

NetID นักศึกษาจะลงท้ายด้วย @stu.nida.ac.th โดยมีรายละเอียดของ และวิธีการดำเนินงาน ดังนี้

1 รหัสนักศึกษา 1 รหัส จะมี NetID 1 บัญชี

2 นักศึกษาจะได้รับ NetID เมื่อขึ้นทะเบียนเป็นนักศึกษา และหากไม่มีการชำระค่าธรรมเนียมการศึกษาเมื่อสิ้นภาคการศึกษาแรกที่ขึ้นทะเบียน NetID จะถูกยกเลิก

3 นักศึกษาที่ได้รับการขึ้นทะเบียนเป็นนักศึกษาก่อนปีการศึกษา 2564 ภาคเรียนที่ 2 จะมีรูปแบบ NetID เป็น name.sur@stu.nida.ac.th และสำหรับนักศึกษาที่ขึ้นทะเบียนตั้งแต่ปีการศึกษา 2564 ภาคเรียนที่ 2 เป็นต้นมาจะมีรูปแบบ NetID เป็น StudentID@stu.nida.ac.th เช่น642xxxxxx@stu.nida.ac.th เป็นต้น

4 นักศึกษาที่ต้องการเปลี่ยนอีเมลสำรอง สามารถดำเนินการผ่านระบบทะเบียนนักศึกษา (https://reg.nida.ac.th/) หรือแจ้งที่คณะเพื่อดำเนินการเปลี่ยน

5 กรณีลืมรหัสผ่าน หรือต้องการเปลี่ยนรหัสผ่านสามารถดำเนินการผ่านเว็บไซต์ https://ams.nida.ac.th/

6 เมื่อสำเร็จการศึกษาแล้ว ข้อกำหนดการใช้งานเป็นไปตาม ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

3.2.1.2 NetID บุคลากร

NetID ของบุคลากรจะลงท้ายด้วย @nida.ac.th โดยมีรายละเอียด และวิธีการดำเนินงานดังนี้

1 บุคลากรขอมี NetID ได้โดยดาวน์โหลดแบบฟอร์มการขอใช้บริการเทคโนโลยีสารสนเทศที่เว็บไซต์ https://idt.nida.ac.th/ แล้วกรอกแบบฟอร์มส่งผ่านระบบ e-doc ไปที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ทั้งนี้ NetID จะสร้างได้ เมื่อบุคลากรได้ทำสัญญาจ้างและทางกองบริหารและพัฒนาทรัพยากรบุคคลได้บันทึกข้อมูลในระบบฐานข้อมูลบุคลากรเรียบร้อยแล้ว

2 NetID บุคลากรสร้างผ่านระบบ AMS

3 บุคลากรที่ต้องการเปลี่ยนอีเมลสำรอง สามารถแจ้งได้ที่กองบริหารและพัฒนาทรัพยากรบุคคล

4 กรณีลืมรหัสผ่าน หรือต้องการเปลี่ยนรหัสผ่านสามารถดำเนินการผ่านเว็บไซต์ https://ams.nida.ac.th/

5 กรณีบุคลากร ลาออก แล้วเข้าใหม่ ระบบ AMS จะเปิดการใช้งาน NetID บุคลากรนั้นอัตโนมัติโดยใช้ NetID เดิม แต่จะมีการปรับปรุงข้อมูลบุคลากรในระบบ AD ให้เป็นปัจจุบัน เช่น หน่วยงานใหม่ที่สังกัด ผู้ดูแลระบบต้องตรวจสอบและกำหนดสิทธิการใช้งานให้ถูกต้อง

6 บุคลากรที่เกษียณอายุราชการ ข้อกำหนดการใช้งานเป็นไปตาม ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

7 กรณีบุคลากรที่ลาออกจากสถาบัน ข้อกำหนดการใช้งานเป็นไปตาม ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

3.2.1.3 NetID สำหรับอาจารย์พิเศษ

NetID อาจารย์พิเศษมีรูปแบบขึ้นต้นด้วย si- ตามด้วยชื่อ.นามสกุล และลงท้ายด้วย @nida.ac.th (si-name.sur@nida.ac.th) โดยมีรายละเอียด และวิธีการดำเนินงาน ดังนี้

1 หน่วยงาน คณะ/สำนัก สามารถขอรับบริการได้โดยกรอกแบบฟอร์มที่เว็บไซต์ https://idtform.nida.ac.th/ (แบบฟอร์มการขอบัญชีผู้ใช้งานสำหรับอาจารย์พิเศษ) แล้วส่งผ่านระบบ e-doc ไปที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2 กำหนดสิทธิการใช้งานให้เป็นไปตามข้อกำหนดการใช้งานเป็นไปตาม ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

3 กรณีอาจารย์พิเศษลืมรหัสผ่าน หรือต้องการเปลี่ยนรหัสผ่านสามารถดำเนินการผ่านเว็บไซต์ https://acm.nida.ac.th/

4 NetID อาจารย์พิเศษ สร้างโดยตรงที่เครื่องแม่ข่าย Active Directory

3.2.1.4 NetID สำหรับหน่วยงาน หรือหลักสูตร (บัญชีอีเมลหน่วยงานหรือหลักสูตร)

NetID หน่วยงานมีรูปแบบเป็นชื่ออีเมลที่ต้องการลงท้ายด้วย @nida.ac.th เช่น idt@nida.ac.th โดยมีรายละเอียด และวิธีการดำเนินงาน ดังนี้

1 หน่วยงาน คณะ/สำนัก สามารถขอรับบริการได้โดยกรอกแบบฟอร์มที่เว็บไซต์ https://idtform.nida.ac.th/ (แบบฟอร์มการขออีเมลกลางสำหรับหน่วยงานหรือหลักสูตร) แล้วส่งผ่านระบบ e-doc ไปที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศ

2 NetID หน่วยงานสามารถใช้บริการสารสนเทศ Microsoft 365 เท่านั้น

3 กำหนดสิทธิการใช้งานให้เป็นไปตามข้อกำหนดการใช้งานเป็นไปตาม ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365

4 กรณีลืมรหัสผ่าน หรือต้องการเปลี่ยนรหัสผ่านสามารถดำเนินการผ่านเว็บไซต์ https://ams.nida.ac.th/ หากเป็นการลืมรหัสผ่านระบบจะส่งอีเมลไปยังอีเมลสำรองของผู้รับผิดชอบบัญชี

5 มีผู้รับผิดชอบบัญชีได้เพียง 1 ท่าน โดยผู้รับผิดชอบบัญชีเป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

6 หากมีการเปลี่ยนแปลงผู้รับผิดชอบบัญชีอีเมลกลางสำหรับหน่วยงานหรือหลักสูตร หน่วยงานต้องทำบันทึกแล้วส่งผ่านระบบ e-doc ไปที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศเพื่อดำเนินการเปลี่ยนผู้รับผิดชอบ

3.2.1.5 NetID สำหรับ บุคคลภายนอกที่ใช้งานอินเทอร์เน็ตแบบชั่วคราว เช่น ผู้เข้าอบรม/สัมมนา เจ้าหน้าที่บริษัท(Outsource)

NetID สำหรับบุคคลภายนอกที่ใช้งานอินเทอร์เน็ตแบบชั่วคราว จะลงท้ายด้วย @guest.nida.ac.th โดยมีรายละเอียด และวิธีการดำเนินงาน ดังนี้

1 หน่วยงาน คณะ/สำนัก สามารถขอรับบริการได้โดยกรอกแบบฟอร์มที่เว็บไซต์ https://idtform.nida.ac.th/ (แบบฟอร์มการขอใช้อินเทอร์เน็ตแบบชั่วคราว), แบบฟอร์มการขอรับบริการ VPN แล้วส่งผ่านระบบ e-doc ไปที่สำนักเทคโนโลยีดิจิทัลและสารสนเทศ
2 สร้างโดยตรงที่เครื่องแม่ข่าย Acticve Directory guest.nida.ac.th
3 กำหนดช่วงเวลาการใช้งานตามที่แจ้งในแบบฟอร์ม
4 สามารถใช้เครือข่ายสถาบันผ่าน WiFi, LAN, VPN เท่านั้น ไม่สามารถใช้บริการ Microsoft 365 ได้

3.2.2 ทบทวนสิทธิการใช้งาน อย่างน้อยปีละ 1 ครั้ง

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ทำการทบทวนสิทธิการใช้งาน Microsoft 365 และบัญชีผู้ใช้งานอินเทอร์เน็ตแบบชั่วคราวสำหรับเจ้าหน้าที่บริษัท (Outsource) อย่างน้อยปีละ 1 ครั้ง

3.3 เงื่อนไข ข้อสังเกต ข้อควรระวัง สิ่งที่ควรคำนึงในการปฏิบัติงาน

การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 นั้นมีเงื่อนไข ข้อสังเกต ข้อควรระวัง สิ่งที่ควรคำนึงในการปฏิบัติงานดังนี้

1 การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 และบัญชีผู้ใช้งานประเภทอื่นที่สามารถเข้าถึงเครือข่ายระบบสารสนเทศของสถาบัน จะต้องดำเนินการภายใต้ประกาศ ข้อกำหนดและคู่มือการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 อย่างเคร่งครัด เพื่อให้มั่นใจได้ว่า

บัญชีผู้ใช้งานมีความถูกต้อง และมีความมั่นคงปลอดภัยต่อระบบเครือข่าย และระบบสารสนเทศของสถาบัน

2 ผู้ปฏิบัติงานที่มีหน้าที่ในการบริหารจัดการ และควบคุมการใช้งานต้องให้ความสำคัญ และตระหนักในข้อมูลส่วนบุคคล ไม่เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ

3 ผู้ปฏิบัติงานที่มีหน้าที่ในการบริหารจัดการ และควบคุมการใช้งานบัญชีผู้ใช้งาน Microsoft 365 และบัญชีผู้ใช้งานประเภทอื่นที่สามารถเข้าถึงเครือข่ายระบบสารสนเทศของสถาบัน ต้องมีความรู้ความเข้าใจในการบริหารจัดการบัญชีผู้ใช้งาน ศึกษา ทำความเข้าใจในประกาศ ข้อกำหนดที่อาจมีการเปลี่ยนแปลง และปฏิบัติตามอย่างเคร่งครัด

4 ต้องทำการทบทวนบัญชีผู้ใช้งานประจำปีอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าผู้ที่มีสิทธิเท่านั้นที่จะสามารถเข้าถึงระบบเครือข่ายสารสนเทศของสถาบันได้

5 ต้องให้สิทธิการใช้งานที่ถูกต้องแก่บัญชีผู้ใช้งานแต่ละประเภท เพื่อป้องกันการเข้าถึงระบบเครือข่ายสารสนเทศของสถาบันโดยไม่ได้รับอนุญาต

3.4 แนวคิด/ งานวิจัยที่เกี่ยวข้อง

ในการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผู้เขียนได้ศึกษาแนวคิด และงานวิจัยที่เกี่ยวข้องดังนี้

3.4.1 แนวคิดการทำงานโดยใช้ PDCA (Plan Do Check Act)

3.4.2 งานวิจัยหลักการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540

3.4.1 แนวคิดการทำงานโดยใช้ PDCA (Plan Do Check Act)

NetID นอกจากจะใช้ในการล็อกอินเพื่อเข้าใช้งานระบบ Microsoft 365 แล้ว ยังสามารถใช้ในการล็อกอินเพื่อเข้าใช้งานระบบสารสนเทศต่างๆของสถาบัน ผู้ปฏิบัติงานที่มีหน้าที่ในการบริหารจัดการบัญชีผู้ใช้งาน จำเป็นต้องมีหลักในการทำงานเพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปด้วยความถูกต้อง เรียบร้อย นำมาซึ่งความปลอดภัยของระบบสารสนเทศต่างๆของสถาบัน โดยใช้แนวคิดในการปฏิบัติงานตามหลัก PDCA ดังนี้

เว็บไซต์ https://www.sakid.app/ (2565) ได้เขียนบทความในหมวด Coporate Wellness เรื่อง PDCA คืออะไร รู้จักหลักการที่ทำให้งานของคุณมีประสิทธิภาพยิ่งขึ้น ดังนี้

PDCA คือวงจรที่ช่วยให้การบริหารงานมีคุณภาพยิ่งขึ้น ช่วยแก้ปัญหาได้อย่างตรงจุด ผ่านองค์ประกอบ 4 ขั้นตอนได้แก่ Plan Do Check Act ซึ่งเครื่องมือนี้เป็นกระบวนการที่จะทำให้การปรับปรุงการทำงานขององค์กรมีระบบยิ่งขึ้น เพื่อเป้าหมายสำคัญคือการแก้ปัญหาอย่างยั่งยืน และเกิดการพัฒนาอย่างต่อเนื่อง

ต้นกำเนิดของ PDCA

PDCA หรือ วงจรเดมิง (Deming Cycle) กำเนิดขึ้นโดย เอ็ดเวิร์ด เดมิง (Edwards Deming) วิศวกรและศาสตราจารย์ชาวอเมริกันที่ทำงานอยู่ในประเทศญี่ปุ่น เครื่องมือนี้ยังมีอีกชื่อเรียกคือ วงจรชูฮาร์ต (Shewhart Cycle) ซึ่งเขาได้ตั้งชื่อตาม วอลเตอร์ ชูฮาร์ต (Walter Shewhart) นักสถิติที่ทุกคนต่างยกย่องให้เป็นบิดาแห่งการควบคุมคุณภาพสมัยใหม่

PDCA เกิดขึ้นมาในช่วง1950’s โดยในการบรรยายที่เผยแพร่เครื่องมือนี้ครั้งแรก เขาได้อธิบายด้วยวงจรแบบง่าย ๆ อย่าง Plan Do Check Act คนจึงคุ้นชินกับ PDCA เป็นส่วนใหญ่ แต่มีเกร็ดข้อมูลเล็กน้อยที่บอกว่าจริง ๆ ในส่วนของ Check แรกเริ่มเดิมทีเดมิงอยากให้เป็น ‘การศึกษา’ หรือ ‘Study’ เพราะเขาให้ความสำคัญกับการวิเคราะห์หรือศึกษาผลลัพธ์มากกว่าแค่ตรวจสอบเฉย ๆ แต่เมื่อหลาย ๆ คนนำไปประยุกต์ใช้ก็ทำให้ PDCA กลายเป็นที่นิยมไป เพราะสุดท้ายแล้วความตั้งใจของเดมิงก็คืออยากให้วงจรนี้ทำซ้ำได้หลาย ๆ ครั้ง เพื่อคอยเช็กหรือศึกษาปัญหาได้ซ้ำ ๆ นั่นเอง

ความหมายของ PDCA

P – Plan : การวางแผน

ก่อนจะแก้ไขปัญหาใด ๆ การวางแผนเป็นเรื่องสำคัญ ขั้นตอนแรกจึงเป็นเรื่องของการวางแผนนั่นเอง ขั้นตอนนี้เป็นขั้นตอนที่ต้องคิดอย่างรอบคอบ วางแผนอย่างครอบคลุมตั้งแต่เริ่มต้นกระบวนการจนสิ้นสุด เช่น ปัญหาคืออะไร ใครเป็นคนรับผิดชอบ จะค้นหาข้อมูลและทดลองแก้ไขอย่างไร ไปจนถึงใช้ตัวชี้วัดใดในการประเมินผล จนกระทั่งปลายทางของขั้นตอนนี้ต้องออกมาเป็นแผนการดำเนินงานหรือ Action Plan ให้ได้

D – DO : การลงมือทำ

หลังจากวางแผนอย่างรัดกุม ต่อมาจึงเป็นการลงมือทำ โดยอาจเริ่มต้นจากการดำเนินการกับทีมน้ำร่อง ในโปรเจ็กต์เล็ก ๆ ก่อน เพื่อป้องกันความผิดพลาดหรือความเสียหาย และเมื่อลงมือทำก็

จะต้องทำตามแผนดำเนินการอย่างรอบคอบ คอยสังเกตความเปลี่ยนแปลง หรือปัญหาใหม่ที่อาจเกิดขึ้นได้ ซึ่งเป็นเรื่องปกติ

C – Check : การตรวจสอบ

เมื่อปฏิบัติตามแผนมาเรื่อบ ๆ ระหว่างทางการทำตามแผน จะต้องมีการตรวจสอบปัญหาหรือผลกระทบอย่างละเอียด สังเกตสิ่งที่เกิดขึ้นว่าเป็นไปตามตัวชี้วัดหรือไม่ เพื่อให้สามารถแก้ปัญหาได้อย่างรวดเร็วและตรงจุด

A – Act : การปฏิบัติเชิงนโยบาย

หลังจากปฏิบัติตามแผนและตรวจสอบอย่างรัดกุม จนไม่พบปัญหาใด ๆ แล้ว จึงจะไปต่อกับขั้นปฏิบัติให้เป็นแบบแผนหรือเป็นนโยบาย โดยนำแผนนั้นมาประยุกต์ใช้กับคนส่วนใหญ่ในองค์กร อาจจะผ่านการอบรม อีเมล์แจ้งข่าว หรือการประชุมใหญ่ โดยขั้นตอนนี้ต้องการปฏิบัติตามอย่างเคร่งครัดเพื่อให้นโยบายได้ประสิทธิภาพจนเห็นการเปลี่ยนแปลง

ประโยชน์ของการทำ PDCA

- ช่วยตรวจสอบปัญหาได้อย่างตรงจุด
- ทำให้การแก้ไขปัญหาเป็นไปอย่างมีประสิทธิภาพ
- เกิดการปรับปรุงพัฒนาอย่างต่อเนื่อง
- สามารถตรวจสอบและทดลองได้เรื่อย ๆ เพื่อหาวิธีที่ดีที่สุด
- ลดความเสี่ยงในการจัดการ เนื่องจากสามารถทดลองกับทีมเล็ก ๆ ได้

ข้อจำกัดของ PDCA

- ผู้นำหรือหัวหน้าทีมต้องตัดสินใจอย่างเด็ดขาด เพราะ PDCA คือเครื่องมือที่เป็นวงจรไม่สิ้นสุด
- ใช้ระยะเวลาในการพัฒนานาน ไม่เหมาะกับการตัดสินใจหรือโปรเจ็กต์ที่เร่งด่วน

สรุป

เมื่อองค์กรเกิดปัญหา การวางแผนแก้ไขปัญหา ทดลองลงมือทำ คอยตรวจสอบ และนำไปปรับในระดับนโยบาย จะช่วยให้การบริหารงานในองค์กรมีประสิทธิภาพมากขึ้น ซึ่ง PDCA ไม่จำเป็นต้องใช้กับปัญหาใหญ่ ๆ เท่านั้น แม้แต่การพัฒนาตัวเองก็สามารถนำเครื่องมือนี้ไปใช้ได้เช่นกัน

แน่นอนว่าทุกการเปลี่ยนแปลง และระหว่างทางในการแก้ไขปัญหาย่อมพบเจออุปสรรคจนอาจย่อท้อ เสียกำลังใจ หรืออาจทำให้สุขภาพของคนในองค์กรนั้นย่ำแย่ลง การดูแลสุขภาพกายและใจของพนักงานจึงเป็นเรื่องสำคัญที่ควรทำควบคู่ไปกับการบริหารจัดการ แก้ไขปัญหาเรื่องประสิทธิภาพ

3.4.2 งานวิจัยหลักการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540

เนื่องจากผู้ปฏิบัติงานที่มีหน้าที่ในการบริหารจัดการ และควบคุมการใช้งานสามารถเข้าถึงข้อมูลส่วนบุคคลจึงต้องให้ความสำคัญ และตระหนักในข้อมูลส่วนบุคคล ไม่เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ โดยมีงานวิจัยที่อ้างอิงหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยดังนี้

นพดล นิ่มหมู(2565) ได้ทำการวิจัยเพื่อศึกษาเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยโดยศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540 ผลสรุป ดังนี้

หลักการคุ้มครองข้อมูลส่วนบุคคลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีฐานะเป็นกฎหมายกลาง กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิตินั้น ได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป(GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ แต่สำหรับในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ มุ่งเน้นคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานภาครัฐ โดยกฎหมายทั้งสองฉบับมีความเหมือนและความแตกต่างกันโดยสรุปดังตารางต่อไปนี้

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540
หลักการของกฎหมายเกี่ยวกับข้อมูลข่าวสารและวัตถุประสงค์ของกฎหมาย	ปกปิดเป็นหลัก เปิดเผยเป็นข้อยกเว้น (มุ่งคุ้มครองสิทธิเจ้าของข้อมูล)	เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น(เพื่อความโปร่งใสในการบริหารงานภาครัฐ)
นิยามของข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ	ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย
ผู้ได้รับความคุ้มครอง	บุคคลธรรมดา	บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทย
การกำหนดหน้าที่ ความรับผิดชอบในการให้ความคุ้มครอง	ควบคุมข้อมูลส่วนบุคคล จะต้อง 1 จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลไม่ได้ให้ความยินยอม และมีการกำหนดหลักการห้ามเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ 2 จัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้	หน้าที่ของหน่วยงานรัฐ (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) จะต้อง 1. จัดระบบข้อมูลข่าวสารส่วนบุคคล เท่าที่เกี่ยวข้องและจำเป็นตามวัตถุประสงค์ และต้องยกเลิกเมื่อหมดความจำเป็น 2. การจัดเก็บข้อมูลให้พยายามจัดเก็บจากเจ้าของโดยตรง

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540
	เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจ 3 จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา 4 หน้าที่แจ้งเหตุ กล่าวคือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล	3. จัดให้มีการตรวจสอบและแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ 4. จัดระบบการรักษาความปลอดภัยให้แก่ระบบข้อมูลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายกับเจ้าของข้อมูล 5. แจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้
การเปิดเผยข้อมูลส่วนบุคคล	ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เว้นแต่กรณีที่ไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26	หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่ มีเหตุตามมาตรา 24 (1)-(9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น
สิทธิของเจ้าของข้อมูล	มีการกำหนดรับรองสิทธิไว้มากมายและกว้างขวางและสอดคล้องกับหลักการสากล เช่น สิทธิที่จะได้รับการแจ้ง (The Right to be Informed), สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน	สิทธิที่กำหนดให้แก่เจ้าของข้อมูลข่าวสารส่วนบุคคลคือ มีสิทธิขอตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตน และมีสิทธิ

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540
	(The Right of Access), สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification),สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to Be Forgotten/ The Right to Erasure), สิทธิที่จะจำกัดการประมวลผล (The Right to Restrict Processing), สิทธิที่จะโอนย้ายข้อมูล(The Right to Data Portability) และสิทธิที่จะคัดค้าน(The Right to Object)	ขอให้แก้ไขเปลี่ยนแปลงให้ถูกต้อง
บทกำหนดโทษ	มีบทกำหนดโทษชัดเจนและรุนแรง	ไม่มีบทกำหนดโทษที่ชัดเจน

ตารางที่ 3-1 : ตารางเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

3.5. วิธีการทำให้ผู้รับบริการมีความพึงพอใจ และวิธีประเมินผลการปฏิบัติงาน

สำนักเทคโนโลยีดิจิทัลและสารสนเทศมีการส่งแบบประเมินความพึงพอใจในการรับบริการผ่านช่องทางอีเมลของผู้ขอรับบริการภายหลังจากได้ปฏิบัติงานสำเร็จแล้ว และนำผลที่ได้มาประเมินเพื่อปรับปรุงการให้บริการให้ดียิ่งขึ้น

3.6. จรรยาบรรณ/ คุณธรรม/ จริยธรรมในการปฏิบัติงาน

การปฏิบัติงานในสถาบันบัณฑิตพัฒนบริหารศาสตร์ ซึ่งเป็นสถาบันการศึกษาที่อยู่ในกำกับของรัฐ ผู้ปฏิบัติงานจะต้องมีจรรยาบรรณ คุณธรรม และจริยธรรมในการปฏิบัติงาน โดยสถาบันได้กำหนดจรรยาบรรณของบุคลากรไว้ในข้อบังคับสถาบันบัณฑิตพัฒนบริหารศาสตร์ ว่าด้วยจรรยาบรรณของบุคลากรสถาบัน พ.ศ.2552 หมวด 2 ซึ่งขอเสนอในส่วนที่เกี่ยวข้องกับการปฏิบัติงาน ดังนี้

1) บุคลากรพึงเป็นผู้ที่ยึดมั่นและยืนหยัดทำในสิ่งที่ดี ถูกต้อง เป็นธรรม และถูกกฎหมาย
2) บุคลากรพึงปฏิบัติหน้าที่อย่างเต็มกำลังความสามารถ รอบคอบ ขยันหมั่นเพียร ถูกต้องสมเหตุสมผล โปร่งใสสามารถตรวจสอบได้ และไม่มีผลประโยชย์ทับซ้อน
3) บุคลากรพึงพัฒนาตนเองให้มีคุณธรรม จริยธรรม ปราศจากอคติ ไม่เลือกปฏิบัติอย่างไม่เป็นธรรม
4) บุคลากรพึงประพฤติตนให้เหมาะสมกับการเป็นแบบอย่างที่ดี และเป็นที่น่าเชื่อถือของบุคคลทั่วไป
5) บุคลากรพึงมุ่งผลสัมฤทธิ์ของงาน เพิ่มพูนความรู้ ความสามารถและทักษะในการทำงาน เพื่อให้การปฏิบัติหน้าที่มีประสิทธิภาพและประสิทธิผลยิ่งขึ้น
6) ตรงต่อเวลา อุทิศเวลาให้แก่สถาบัน ไม่ทอดทิ้งหรือละทิ้งหน้าที่ของตนในการปฏิบัติงาน
7) รักษาความลับที่สถาบันต้องดำเนินการตามกฎหมายหรือธรรมเนียมปฏิบัติ
8) บุคลากรพึงเคารพและปฏิบัติตามคำสั่งของผู้บังคับบัญชาซึ่งสั่งในหน้าที่โดยชอบด้วยกฎหมาย และระเบียบของสถาบันโดยปราศจากอคติ
9) บุคลากรพึงให้ความร่วมมือช่วยเหลือผู้ร่วมงานทั้งในด้านการให้ความคิดเห็น และการแก้ปัญหาร่วมกัน การเสนอแนะในสิ่งที่เห็นว่าจะเป็นประโยชน์ต่อการพัฒนางานใน

10) ความรับผิดชอบ รวมทั้งให้ความร่วมมือในการเข้าร่วมกิจกรรมต่าง ๆ ที่เป็นประโยชน์ต่อสถาบัน
11) บุคลากรพึงให้บริการอย่างเต็มความสามารถด้วยความเป็นธรรม เอื้อเฟื้อ มีน้ำใจ และใช้กิริยาวาจาที่สุภาพอ่อนโยน
12) บุคลการพึงละเว้นจากการเปิดเผยความลับของนักศึกษาที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจโดยมิชอบจนก่อให้เกิดความเสียหายแก่นักศึกษาหรือผู้รับบริการ
13) บุคลากรพึงละเว้นจากการเรียก รับ หรือยอมจะรับทรัพย์สินหรือประโยชน์อื่นใดจากนักศึกษาหรือผู้รับบริการเพื่อกระทำหรือไม่กระทำการใ

บทที่ 4
เทคนิคในการปฏิบัติงาน

ปัจจุบันสถาบันใช้บริการ NetID ของบริษัท Microsoft มีการบริหารจัดการบัญชีผู้ใช้งานผ่านระบบ AMS :โดยประเภทผู้ใช้งานหลักได้แก่ นักศึกษา บุคลากร หน่วยงาน ซึ่งการบริหารจัดการบัญชีผู้ใช้แต่ละประเภทมีรายละเอียดและขั้นตอนการดำเนินการที่แตกต่างกัน ดังนั้นผู้ดูแลระบบจึงต้องมีความรู้ความเข้าใจในกระบวนการดำเนินการต่างๆที่เกี่ยวข้องเพื่อให้การบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบ AMS เป็นไปด้วยความรวดเร็ว และถูกต้อง โดยผู้เขียนได้แบ่งกระบวนการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 ผ่านระบบ AMS เป็น 2 กระบวนงานดังนี้

4.1 การบริหารจัดการ NetID

4.2 การบริหารจัดการกลุ่มผู้ใช้งาน และการให้สิทธิ์ระบบที่ให้บริการ

4.1 การบริหารจัดการ NetID

การบริหารจัดการ NetID ผ่านระบบ AMS นั้น รองรับประเภทของผู้ใช้งาน 4 ประเภท ได้แก่

4.1.1 การบริหารจัดการ NetID นักศึกษา

4.1.2 การบริหารจัดการ NetID บุคลากร

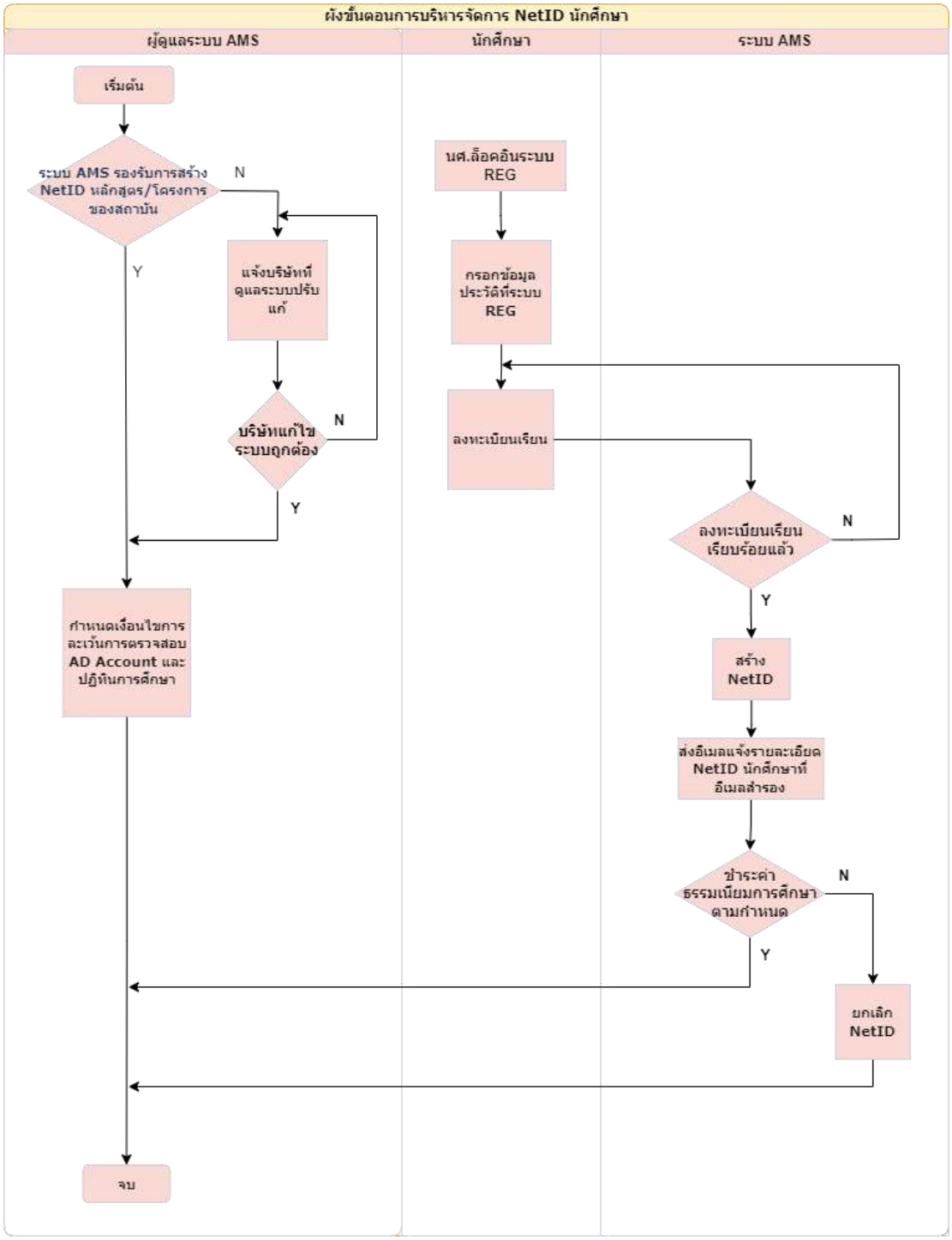
4.1.3 การบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร

4.1.4 การบริหารจัดการ NetID กรณีศิษย์เก่า

4.1.1 การบริหารจัดการ NetID ของนักศึกษา

NetID นักศึกษา (@stu.nida.ac.th) เป็นการสร้างจากระบบ AMS แบบอัตโนมัติตามเงื่อนไขที่กำหนดไว้ ผู้ดูแลระบบจะต้องมีความรู้ความเข้าใจในกระบวนการดำเนินการ เพื่อให้การบริหารบัญชีผู้ใช้งานของนักศึกษาถูกต้อง และพร้อมใช้งานอย่างมีประสิทธิภาพ โดยมีผังขั้นตอน และกระบวนการบริหารจัดการ NetID นักศึกษาดังนี้

ผังขั้นตอนการบริหารจัดการ NetID นักศึกษา



ภาพที่ 4-1 : ผังขั้นตอนการบริหารจัดการ NetID นักศึกษา

กระบวนการบริหารจัดการ NetID นักศึกษา

กระบวนการบริหารจัดการ NetID นักศึกษาเป็นกระบวนการในการได้มาของ NetID นักศึกษา ซึ่ง NetID จะสร้างเมื่อนักศึกษาได้ลงทะเบียนเรียนเรียบร้อยแล้ว และสิทธิในการใช้งานเป็นไปตามเงื่อนไขที่กำหนดไว้ในระบบ AMS โดยแบ่งเป็น 2 กระบวนการดังนี้

1. การตรวจสอบการทำงานของระบบ การกำหนดเงื่อนไขละเว้นการตรวจสอบค่าธรรมเนียมการศึกษา และการยกเลิก NetID
2. การสร้าง NetID นักศึกษา

1. การตรวจสอบการทำงานของระบบ การกำหนดเงื่อนไขละเว้นการตรวจสอบค่าธรรมเนียมการศึกษา และการยกเลิก NetID

ผู้ดูแลระบบ AMS ต้องเป็นผู้กำหนดเงื่อนไขที่ใช้ในการสร้าง NetID ของนักศึกษาประสานงานกับกองบริการ คณะ และบริษัทที่ดูแลระบบเพื่อให้ระบบสามารถทำงานได้ถูกต้องรวดเร็วดังนี้

1) ตรวจสอบระบบ AMS ว่ารองรับการสร้าง NetID ของนักศึกษาในทุกหลักสูตร/โครงการหรือไม่ หากพบว่าระบบยังไม่รองรับให้แจ้งบริษัทที่ดูแลระบบเพื่อทำการปรับปรุงระบบให้สามารถทำงานได้ถูกต้อง

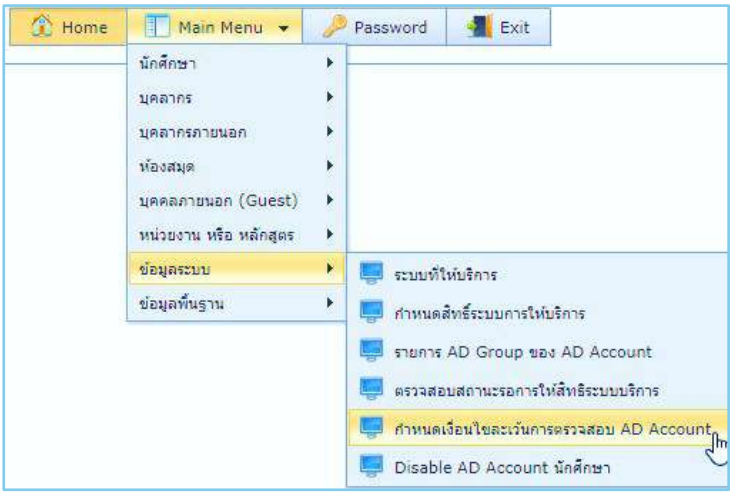
   ข้อสังเกต ข้อควรระวัง : หากคณะมีการเพิ่มหลักสูตรหรือโครงการใหม่ ระบบ AMS จะไม่รองรับการสร้าง NetID ผู้ดูแลระบบต้องประสานงานกับกองบริการการศึกษา คณะ เพื่อขอรายละเอียดและแจ้งให้บริษัทปรับแก้ระบบให้ทำงานได้ถูกต้อง

2) กำหนดเงื่อนไขละเว้นการตรวจสอบค่าธรรมเนียมการศึกษา และปฏิทินการศึกษาเพื่อให้ระบบทำการตรวจสอบการชำระค่าธรรมเนียมการศึกษาตามเงื่อนไขที่กำหนดเพื่อยกเลิก NetID

   ข้อสังเกต ข้อควรระวัง : หลักสูตรที่ละเว้นการตรวจสอบ เช่น หลักสูตรปริญญาโท สมทบ พิเศษ (MOU) ของคณะพัฒนาการเศรษฐกิจ เนื่องจากค่าธรรมเนียมการศึกษาต้องรอสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังโอนมา ไม่สามารถกำหนดวันที่แน่นอนได้

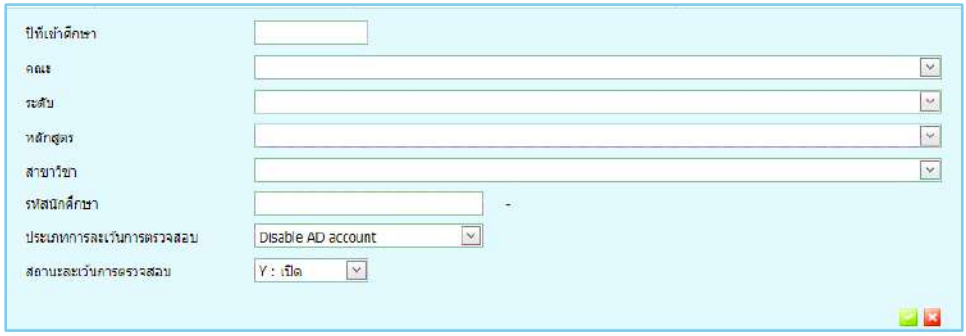
การกำหนดเงื่อนไขละเว้นการตรวจสอบค่าธรรมเนียมการศึกษา มีขั้นตอนการดำเนินการดังนี้

1) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
2) กำหนดเงื่อนไขละเว้นการตรวจสอบการชำระค่าธรรมเนียมการศึกษาผ่านเมนู ข้อมูลระบบ



ภาพที่ 4-2 : การกำหนดเงื่อนไขการละเว้นการตรวจสอบ AD Account

3) ใส่รายละเอียดที่ต้องการละเว้นการตรวจสอบ AD Account โดยต้องเลือกปีที่เข้าศึกษาและกำหนดรายละเอียดที่ต้องการละเว้น สามารถกำหนดเป็นรายคน หรือหลักสูตรได้
4) เลือกประเภทเป็น Disable AD account และ สถานะละเว้นการตรวจสอบเป็น Y



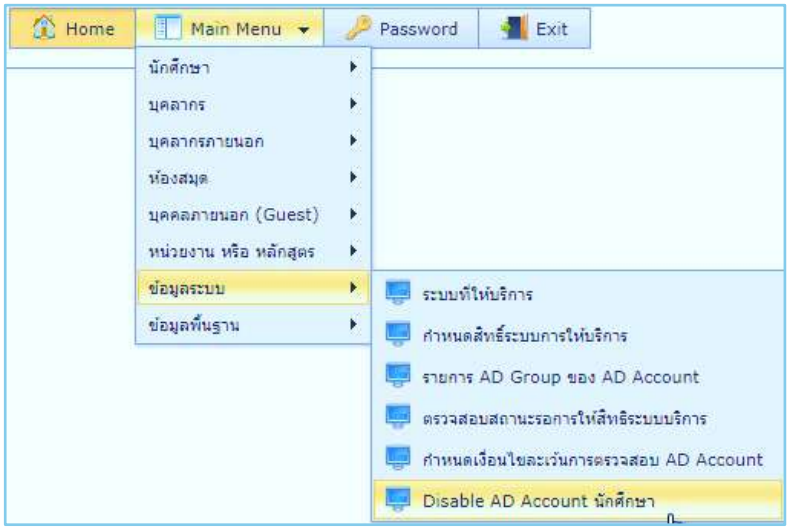
ภาพที่ 4-3 : รายละเอียดเพื่อกำหนดเงื่อนไขการละเว้นการตรวจอบ AD Account

ข้อสังเกต ข้อควรระวัง : หากผู้ดูแลระบบลืมกำหนดเงื่อนไขหลักสูตรที่ต้องการละเว้นการตรวจสอบเมื่อสิ้นภาคการศึกษาระบบอาจมีการยกเลิก NetID ของนักศึกษาเนื่องจากตรวจสอบข้อมูลจากระบบ REG แล้วยังไม่มีการชำระค่าธรรมเนียมการศึกษา

การยกเลิก NetID

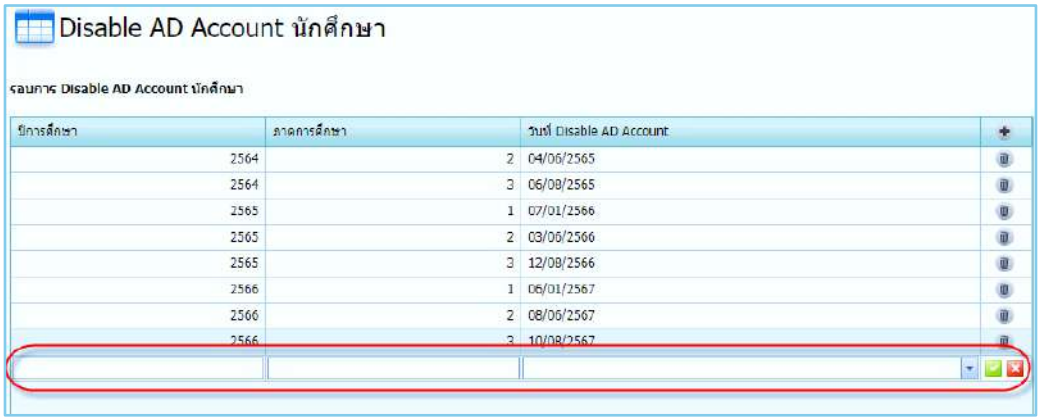
ผู้ดูแลระบบต้องกำหนดปฏิทินการศึกษาแต่ละภาคการศึกษาของปีการศึกษาล่วงหน้า โดยอ้างอิงตามปฏิทินการศึกษาประจำปีของสถาบันเพื่อใช้เป็นเงื่อนไขในการตรวจสอบการยกเลิก NetID หากนักศึกษาไม่ชำระค่าธรรมเนียมการศึกษาภายในระยะเวลาที่กำหนดไว้ โดยมีขั้นตอนดังนี้

1) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
2) เลือก Disable AD Account นักศึกษาผ่านเมนู ข้อมูลระบบ



ภาพที่ 4-4 : การ Disable AD Account นักศึกษา

3) เพิ่มรายการ ปีการศึกษา ภาคการศึกษา และวันที่ Disable AD Account โดยอ้างอิงวันสุดท้ายของภาคการศึกษาบวก 1 วัน ตามปฏิทินการศึกษาของสถาบัน



ภาพที่ 4-5 : เพิ่มราย การ Disable AD Account นักศึกษา

การสร้าง NetID นักศึกษา

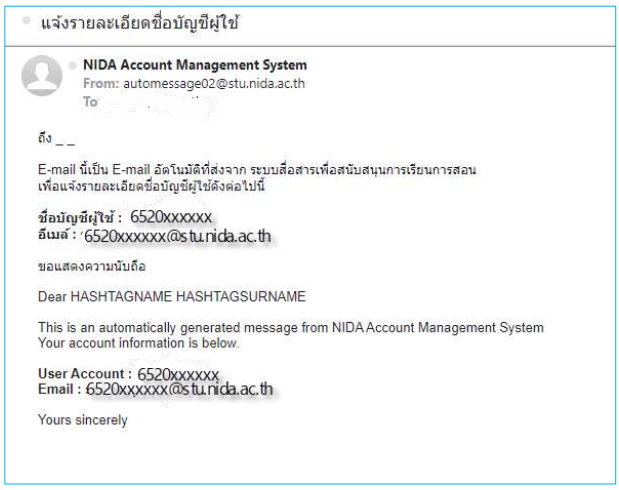
การสร้าง NetID นักศึกษาผ่านระบบ AMS มีกระบวนการดำเนินการดังนี้

1) นักศึกษาใหม่กรอกประวัติ ข้อมูลส่วนตัวที่ระบบบริการการศึกษา (https://reg.nida.ac.th/)

ข้อสังเกต ข้อควรระวัง : ข้อมูลของนักศึกษาที่กรอกในระบบ REG ได้แก่ ชื่อ-นามสกุล (ภาษาอังกฤษ) เลขบัตรประจำตัวประชาชน หรือเลขพาสปอร์ต อีเมลสำรอง โดยข้อมูลดังกล่าวต้องเป็นข้อมูลที่ถูกต้องเนื่องจากเป็นข้อมูลที่ใช้อ้างอิงในการสร้าง NetID และใช้ในกระบวนการจัดการรหัสผ่านของนักศึกษา

2) นักศึกษาลงทะเบียนเรียนภาคการศึกษาแรก
3) ระบบ AMS ตรวจสอบข้อมูลของนักศึกษาจากระบบ REG หากนักศึกษาดำเนินการตามข้อ 1 และ 2 ครบตามข้อกำหนดระบบจะทำการสร้าง NetID
4) ระบบ AMS ส่งอีเมลไปยังอีเมลสำรองของนักศึกษา เพื่อแจ้งรายละเอียด NetID
5) ระบบจะตรวจสอบการชำระค่าธรรมเนียมการศึกษาเมื่อสิ้นภาคการศึกษาแรกที่นักศึกษาได้ลงทะเบียนเรียน หากไม่มีการชำระค่าธรรมเนียมการศึกษาระบบจะทำการยกเลิก NetID ของนักศึกษา

ข้อสังเกต ข้อควรระวัง : หากผู้ดูแลระบบไม่กำหนดวันสุดท้ายของภาคการศึกษาในระบบ AMS ระบบจะไม่ตรวจสอบสถานะการชำระค่าธรรมเนียมการศึกษามีผลให้ NetID นั้นยังสามารถใช้งานต่อไปได้ ขั้นตอนการกำหนดวันสุดท้ายของภาคการศึกษา อ้างอิงหัวข้อ การ Disable Account นักศึกษา


แจ้งรายละเอียดชื่อบัญชีผู้ใช้

NIDA Account Management System
From: automessage02@stu.nida.ac.th
To

ถึง _ _

E-mail นี้เป็น E-mail อัตโนมัติที่ส่งจาก ระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน
เพื่อแจ้งรายละเอียดชื่อบัญชีผู้ใช้ดังต่อไปนี้

ชื่อบัญชีผู้ใช้ : 6520xxxxxx
อีเมล์ : 6520xxxxxx@stu.nida.ac.th

ขอแสดงความนับถือ

Dear HASHTAGNAME HASHTAGSURNAME

This is an automatically generated message from NIDA Account Management System
Your account information is below.

User Account : 6520xxxxxx
Email : 6520xxxxxx@stu.nida.ac.th

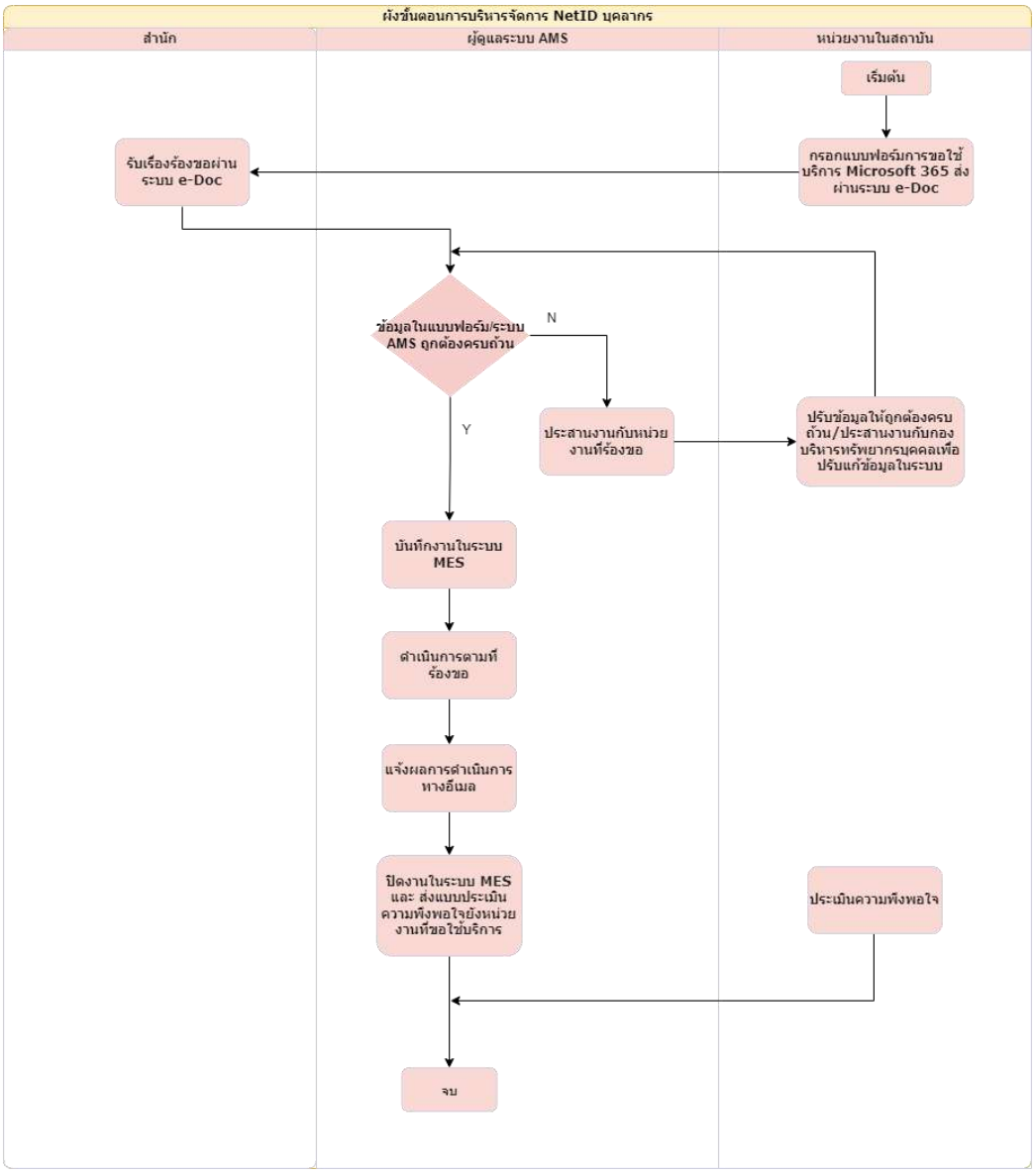
Yours sincerely

ภาพที่ 4-6 : ตัวอย่างอีเมลที่แจ้งรายละเอียด NetID นักศึกษา

4.1.2 การบริหารจัดการ NetID บุคลากร

NetId ของบุคลากร (@nida.ac.th) ใช้เพื่อยืนยันตัวตนในการเข้าใช้งานระบบเครือข่าย และระบบสารสนเทศต่างๆของสถาบัน โดย NetID และจะถูกยกเลิกเมื่อบุคลากรได้ลาออก สำหรับบุคลากรที่เกษียณอายุราชการจะได้รับสิทธิในการใช้งานอีเมล @nida.ac.th และ Microsoft 365 แบบบนคลาวน์ ตามประกาศสถาบันบัน เรื่องการจัดบริการ Microsoft 365 โดยมีผังขั้นตอนการบริหารจัดการ NetID บุคลากร ดังนี้

ผังขั้นตอนการบริหารจัดการ NetID บุคลากร



ภาพที่ 4-7 : ผังขั้นตอนการบริหารจัดการ NetID บุคลากร

กระบวนการบริหารจัดการ NetID บุคลากร

การบริหารจัดการ NetID บุคลากรประกอบด้วย 2 กระบวนการหลักๆ ดังนี้

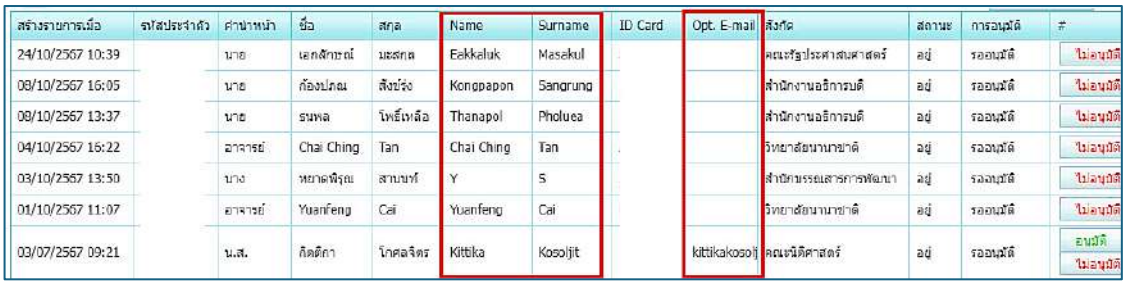
1. การสร้าง NetID บุคลากร
2. การยกเลิก NetID บุคลากร

1. การสร้าง NetID บุคลากร

NetID ของบุคลากร (@nida.ac.th) จะสามารถสร้างได้เมื่อบุคลากรได้ทำสัญญาเข้าทำงานกับสถาบัน และกองบริหารและพัฒนาทรัพยากรบุคคลได้บันทึกข้อมูลบุคลากรนั้นในระบบ MIS แล้ว โดยข้อมูลที่จำเป็นในการสร้าง NetID ของบุคลากรอย่างน้อยต้องประกอบด้วย ชื่อ-นามสกุล(ไทย-อังกฤษ) อีเมลสำรอง หมายเลขบัตรประจำตัวประชาชนหรือหมายเลขพาสปอร์ต หน่วยงานที่สังกัด การสร้าง NetID บุคลากรมีกระบวนการ ดังนี้

1) ผู้ขอรับบริการกรอกแบบฟอร์มการขอใช้บริการเทคโนโลยีสารสนเทศ (ITC001-1) เพื่อขอบัญชีผู้ใช้งาน Microsoft 365 (NetID) ส่งผ่านระบบ e-doc มายังสำนัก
2) ผู้ดูแลระบบตรวจสอบข้อมูลบุคลากรที่ขอ NetID ที่ระบบ AMS หากข้อมูลถูกต้องครบถ้วน ผู้ดูแลระบบจะสามารถคลิก “อนุมัติ” เพื่อให้ระบบสร้างบัญชีผู้ใช้งานได้ หากข้อมูลในระบบไม่ถูกต้อง หรือในระบบยังไม่มีข้อมูลอีเมลสำรอง ผู้ดูแลระบบต้องประสานงานกับหน่วยงานที่บุคลากรใหม่สังกัดเพื่อประสานงานกับกองบริหารทรัพยากรบุคคลในการบันทึก/แก้ไขข้อมูล

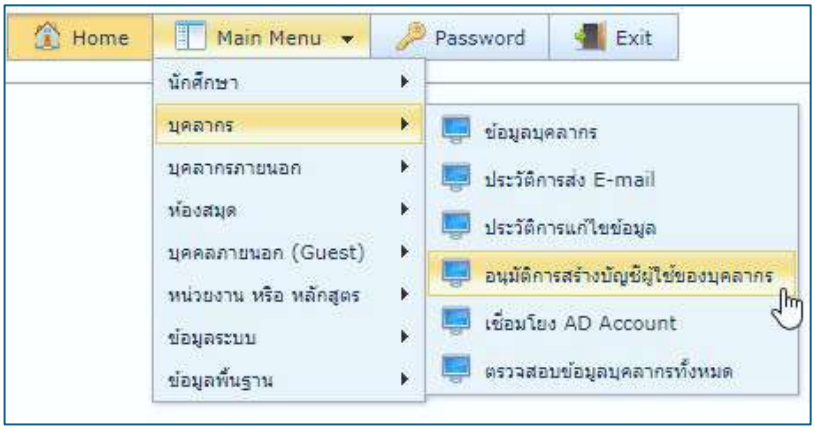
ข้อสังเกต ข้อควรระวัง : ก่อนอนุมัติบัญชีผู้ใช้งาน ผู้ดูแลระบบต้องสังเกต และตรวจสอบข้อมูลบุคลากรที่บันทึกในระบบ โดยเปรียบเทียบกับข้อมูลในแบบฟอร์มการขอใช้บริการเทคโนโลยีสารสนเทศ (ITC001-1) หากข้อมูลไม่ตรงกันให้ตรวจสอบกับผู้ขอรับบริการ เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นในการสร้าง NetID เช่น NetID ที่สร้างไม่ตรงกับชื่อ นามสกุล หรือ ระบบไม่สามารถสร้าง NetID ได้



สร้างรายการเมื่อ	รหัสประจำตัว	คำนำหน้า	ชื่อ	สกุล	Name	Surname	ID Card	Opt. E-mail	สังกัด	สถานะ	การอนุมัติ	#
24/10/2567 10:39		นาย	เอกลักษณ์	มสกุล	Eekkaluk	Masakul			คณะรัฐประศาสนศาสตร์	อยู่	รออนุมัติ	ไม่อนุมัติ
08/10/2567 16:05		นาย	ก้องปภณ	สังข์รัง	Kongpapon	Sangrung			สำนักงานอธิการบดี	อยู่	รออนุมัติ	ไม่อนุมัติ
08/10/2567 13:37		นาย	ธนพล	โพธิ์เหลือ	Thanapol	Pholuea			สำนักงานอธิการบดี	อยู่	รออนุมัติ	ไม่อนุมัติ
04/10/2567 16:22		อาจารย์	Chai Ching	Tan	Chai Ching	Tan			วิทยาลัยนานาชาติ	อยู่	รออนุมัติ	ไม่อนุมัติ
03/10/2567 13:50		นาง	หยาดพิรุณ	สาบขำ	Y	S			สำนักพรรณสารการพัฒนา	อยู่	รออนุมัติ	ไม่อนุมัติ
01/10/2567 11:07		อาจารย์	Yuanfeng	Cai	Yuanfeng	Cai			วิทยาลัยนานาชาติ	อยู่	รออนุมัติ	ไม่อนุมัติ
03/07/2567 09:21		น.ส.	กิตติกา	โกศลจิตร	Kittika	Kosoljit		kittikakosolj	คณะนิติศาสตร์	อยู่	รออนุมัติ	อนุมัติ ไม่อนุมัติ

ภาพที่ 4-8 : ข้อมูลบุคลากรที่รออนุมัติการสร้าง NetID

3) ผู้ดูแลระบบบันทึกงานในระบบ MES
4) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
5) เลือก บุคลากร และเลือก อนุมัติการสร้างบัญชีผู้ใช้ของบุคลากรเพื่อสร้าง NetID บุคลากร



ภาพที่ 4-9 : การอนุมัติการสร้าง NetID ของบุคลากร

6) กำหนด License และ Group -ของบุคลากรบน Microsoft 365 ตามประเภทของบุคลากรปัจจุบัน,กำหนด Group Policy OneDrive และ Group หน่วยงานที่สังกัดเพื่อให้สามารถเข้าถึง Sharepoint ที่มีการกำหนดสิทธิตามหน่วยงานนั้นๆ
7) แจ้งรายละเอียด NetID และการใช้งาน Microsoft 365 ที่อีเมลสำรองของบุคลากร
8) ปิดงานในระบบ MES
9) ส่งแบบประเมินความพึงพอใจในการให้บริการ

****บุคลากรที่ลาออกแล้วเข้าบรรจุใหม่ ระบบ AMS จะทำการเปิดใช้งานบัญชี (Enable Account AD) ให้โดยอัตโนมัติเป็นบัญชีเดิม (NetID เดิม) โดยมีการปรับปรุงข้อมูล เลขประจำตัวบุคลากร และหน่วยงานที่สังกัดให้เป็นปัจจุบัน ผู้ดูแลระบบต้องตรวจสอบความถูกต้องของสิทธิการใช้งาน Microsoft 365(License) และระบบสารสนเทศต่างๆหากไม่ถูกต้องต้องดำเนินการแก้ไขให้ตรงกับสิทธิที่เป็นปัจจุบัน**

ข้อสังเกต ข้อควรระวัง : หากสถาบันมีการปรับโครงสร้างหน่วยงาน ผู้ดูแลระบบจะต้องประสานงานกับบริษัทเพื่อปรับปรุงระบบให้รองรับกับโครงสร้างใหม่ของสถาบันโดยเร่งด่วน มิเช่นนั้นจะส่งผลกระทบกับระบบการบริหารจัดการบัญชีผู้ใช้งาน Microsoft 365 -ของสถาบัน ทำให้ไม่สามารถบริหารจัดการบัญชีผู้ใช้งานได้

2. การยกเลิก NetID บุคลากร

NetID ของบุคลากรจะถูกยกเลิกเมื่อบุคลากรได้ลาออก หากบุคลากรนั้นต้องการใช้งานอีเมล (@nida.ac.th) ต่อ ให้ดำเนินการตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365 การยกเลิก NetID บุคลากรมีกระบวนการดังนี้

1) กองบริหารทรัพยากรบุคคลมีบันทึกแจ้งมายังสำนักเรื่องบุคลากรที่ลาออก หรือหน่วยงานหรือเจ้าของบัญชีกรอกแบบฟอร์มยกเลิกการใช้บริการเทคโนโลยีสารสนเทศ (ITC002-1) เพื่อขอยกเลิกบัญชีผู้ใช้งาน Microsoft 365 (NetID) ส่งผ่านระบบ e-doc มายังสำนัก
2) ผู้ดูแลระบบตรวจสอบข้อมูลบุคลากรที่ลาออกในระบบ AMS กรณีไม่มีข้อมูลในระบบหรือมีข้อสงสัยให้ประสานงานกับหน่วยงานที่บุคลากรสังกัด หรือกองบริหารทรัพยากรบุคคลก่อนดำเนินการ
3) ผู้ดูแลระบบบันทึกงานในระบบ MES
4) ยกเลิกบัญชีผู้ใช้งาน โดยการ Disable Account บน AD และย้าย Account ไปยัง OU ที่เก็บบัญชีผู้ใช้งานที่ลาออก
5) นำสิทธิของบุคลากรที่ลาออกออก ได้แก่ License และ Group บน Microsoft 365
6) ปิดงานในระบบ MES

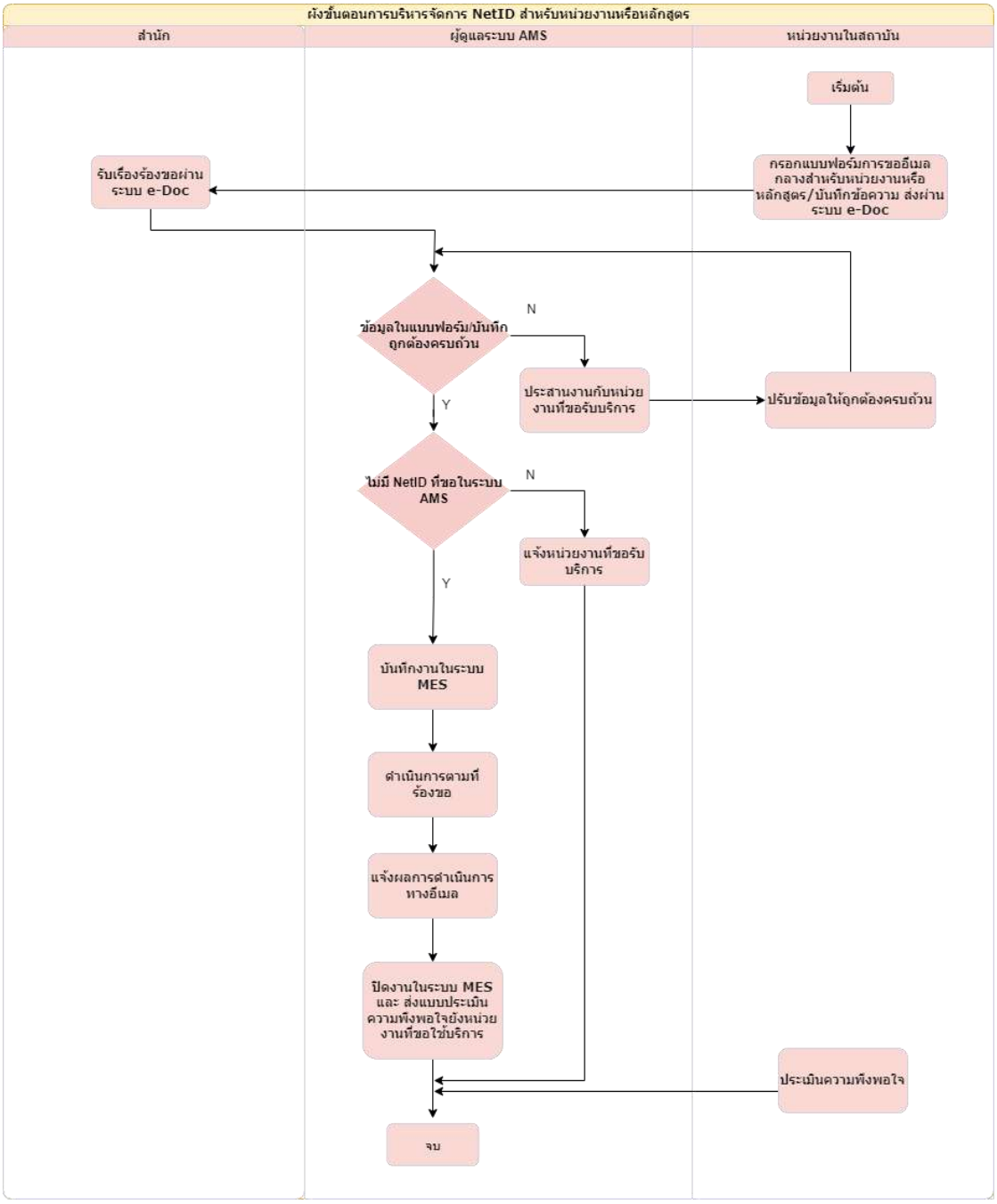
ข้อสังเกต ข้อควรระวัง : หากบุคลากรที่ลาออกแล้วหน่วยงาน หรือกองบริหารทรัพยากรบุคคลไม่แจ้งยกเลิกบัญชีผู้ใช้งานมายังสำนัก ซึ่งอาจพบได้ในกรณีลูกจ้างชั่วคราวของหน่วยงาน บุคลากรนั้นจะยังสามารถเข้าใช้บริการเครือข่าย และระบบสารสนเทศของสถาบันได้ตามปกติ สำนักจึงมีความจำเป็นต้องทบทวนบัญชีผู้ใช้งานประจำปีเพื่อจะได้ยกเลิก NetID ของบุคลากรที่ลาออกต่อไป

4.1.3 การบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร

บัญชีผู้ใช้งานสำหรับหน่วยงานหรือหลักสูตร (@nida.ac.th) เป็นบัญชีอีเมลกลางของหน่วยงานที่ใช้สำหรับติดต่อสื่อสารผ่านช่องทางอีเมลกับหน่วยงานหรือบุคคลภายนอก จะไม่สามารถนำบัญชีอีเมลนี้ไปใช้ยืนยันตัวตนเพื่อเข้าใช้งานระบบสารสนเทศอื่นๆของสถาบันได้นอกจากระบบ Microsoft 365 เท่านั้น

บัญชีประเภทนี้ผู้รับผิดชอบบัญชี เป็นผู้รับทราบนโยบาย และต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม การลืมรหัสผ่าน หรือกำหนดรหัสผ่านใหม่นั้นระบบจะเชื่อมโยงกับอีเมลสำรองของผู้รับผิดชอบบัญชี หากมีการเปลี่ยนแปลงผู้รับผิดชอบบัญชี หน่วยงานต้องแจ้งเปลี่ยนชื่อผู้รับผิดชอบมายังสำนักเพื่อดำเนินการต่อไป การบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตรมีผังขั้นตอนการดำเนินการ ดังนี้

ผังขั้นตอนการบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร



ภาพที่ 4-10 : ผังขั้นตอนการบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร

กระบวนการบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร

กระบวนการบริหารจัดการ NetID สำหรับหน่วยงานหรือหลักสูตร แบ่งเป็น 3 กระบวนการหลักๆ ดังนี้

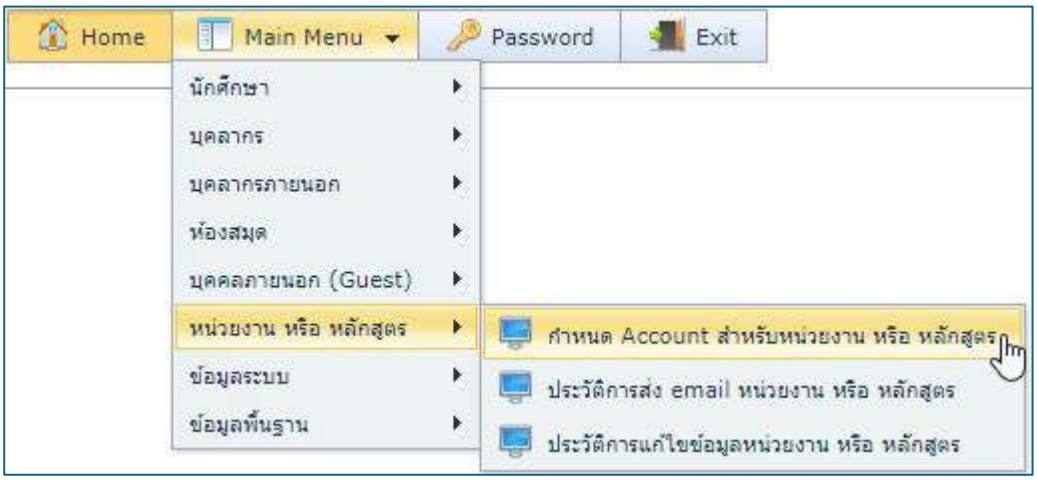
1. การสร้าง NetID สำหรับหน่วยงาน หรือ หลักสูตร
2. การเปลี่ยนผู้รับผิดชอบ NetID สำหรับหน่วยงาน หรือ หลักสูตร
3. การยกเลิก NetID หน่วยงาน หรือ หลักสูตร

1. การสร้าง NetID สำหรับหน่วยงาน หรือ หลักสูตร

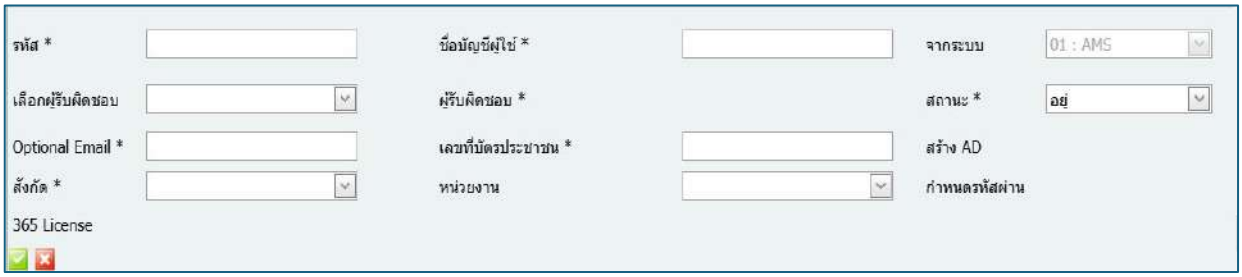
เมื่อหน่วยงานมีความจำเป็นต้องใช้อีเมลกลางในการติดต่อสื่อสาร เช่น อีเมลของหลักสูตร อีเมลของส่วนงาน หรือ โครงการ จะมีกระบวนการในการดำเนินการดังนี้

1) ผู้ขอรับบริการกรอกแบบฟอร์มการขออีเมลกลางสำหรับหน่วยงานหรือหลักสูตร(IDT-FM-IS-006) ส่งผ่านระบบ e-doc มายังสำนัก
2) ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม หากข้อมูลไม่ถูกต้องครบถ้วนให้ประสานงานกับทางหน่วยงานที่ขอรับบริการ
3) ตรวจสอบในระบบ AMS ว่ามี NetID ที่ขอมาในระบบหรือไม่ หากมี NetID นั้นแล้วให้แจ้งหน่วยงานที่ขอรับบริการ
4) ผู้ดูแลระบบบันทึกงานในระบบ MES
5) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
6) เลือก กำหนด Account สำหรับหน่วยงาน หรือ หลักสูตร จากเมนู หน่วยงาน หรือ หลักสูตร แล้วคลิกที่เครื่องหมาย + เพื่อสร้าง NetID หน่วยงาน หรือ หลักสูตร บันทึกข้อมูล ชื่อบัญชีผู้ใช้งาน (ชื่อ NetID สำหรับหน่วยงาน หรือ หลักสูตร) เลือกผู้รับผิดชอบ สังกัด คลิกที่เครื่องหมาย ✓ NetID ที่บันทึกจะยังไม่มีการสร้าง ผู้ดูแลระบบต้องคลิกปุ่ม “สร้าง” หลังรายการ NetID นั้นๆ เพื่อยืนยันการสร้าง และกำหนด Display name ตามที่ผู้ขอรับบริการแจ้งในแบบฟอร์ม

   ข้อสังเกต ข้อควรระวัง : Display name คือ ชื่อที่แสดงของอีเมลกลางนั้นๆ เช่น idt@nida.ac.th : Display name ที่แสดง คือ Information and Digital Technology Center(IDT) ผู้ดูแลระบบจะต้องปรับแก้ Display name ของ NetID หน่วยงาน หรือ หลักสูตรที่ระบบ AD ให้ตรงตามที่หน่วยงานต้องการ



ภาพที่ 4-11 : การสร้าง NetID สำหรับหน่วยงาน หรือ หลักสูตร



ภาพที่ 4-12 : รายละเอียดที่ต้องบันทึกในการสร้าง NetID สำหรับหน่วยงาน หรือ หลักสูตร

7) กำหนด License และ Group Policy OneDrive ของ NetID หน่วยงาน หรือ หลักสูตรบน Microsoft 365 ตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่องการจัดบริการ Microsoft 365
8) แจ้งรายละเอียด NetID และการใช้งาน Microsoft 365 ที่อีเมลผู้รับผิดชอบบัญชี
9) ปิดงานในระบบ MES
10) ส่งแบบประเมินความพึงพอใจในการให้บริการ

ข้อสังเกต ข้อควรระวัง : เมื่อระบบสร้าง NetID สำหรับหน่วยงาน หรือ หลักสูตรเรียบร้อยแล้ว ระบบจะส่งอีเมลไปยังอีเมลสำรองของผู้รับผิดชอบ NetID เพื่อให้กำหนดรหัสผ่านในการใช้งาน ผู้ดูแลระบบควรแจ้ง หรือ สอบถามผู้รับผิดชอบ NetID ทุกครั้งหลังทำการสร้าง NetID สำหรับหน่วยงานหรือหลักสูตร

2. การเปลี่ยนผู้รับผิดชอบ NetID สำหรับหน่วยงาน หรือ หลักสูตร

เมื่อผู้รับผิดชอบ NetID สำหรับหน่วยงาน หรือ หลักสูตรลาออก หรือเกษียณอายุ หรือหน่วยงานต้องการเปลี่ยนผู้รับผิดชอบบัญชีจะมีกระบวนการดำเนินการดังนี้

1) ผู้ขอรับบริการทำบันทึกแจ้งความประสงค์เพื่อขอเปลี่ยนผู้รับผิดชอบ NetID ส่งผ่านระบบ e-doc มายังสำนัก
2) ผู้ดูแลระบบตรวจสอบข้อมูลในบันทึก หากข้อมูลไม่ถูกต้องครบถ้วนให้ประสานงานกับทางหน่วยงานที่ขอรับบริการ
3) ตรวจสอบในระบบ AMS ว่ามี NetID ที่แจ้งมาในระบบหรือไม่ หากไม่มี NetID นั้นให้แจ้งหน่วยงานที่ขอรับบริการ
4) ผู้ดูแลระบบบันทึกงานในระบบ MES
5) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu

11) เลือก กำหนด Account สำหรับหน่วยงาน หรือ หลักสูตร จากเมนู หน่วยงาน หรือ หลักสูตร แล้วค้นหาชื่อ NetID ที่ต้องการเปลี่ยนผู้รับผิดชอบ เลือกผู้รับผิดชอบ เป็นผู้รับผิดชอบ NetID คนใหม่ แล้วคลิกที่เครื่องหมาย ✓ เพื่อยืนยัน
12) แจ้งผลการดำเนินการที่อีเมลผู้รับผิดชอบ NetID คนใหม่
13) ปิดงานในระบบ MES
14) ส่งแบบประเมินความพึงพอใจในการให้บริการ

ข้อสังเกต ข้อควรระวัง : เมื่อเปลี่ยนผู้รับผิดชอบ NetID สำหรับหน่วยงาน หรือ หลักสูตร เรียบร้อยแล้ว ระบบจะส่งอีเมลไปยังอีเมลสำรองของผู้รับผิดชอบ NetID คนใหม่เพื่อให้กำหนดรหัสผ่านในการใช้งาน ผู้ดูแลระบบควรแจ้ง หรือ สอบถามผู้รับผิดชอบ NetID ทุกครั้งเมื่อดำเนินการแล้วเสร็จ

3. การยกเลิก NetID สำหรับหน่วยงาน หรือ หลักสูตร

NetID สำหรับหน่วยงาน หรือ หลักสูตรบางบัญชีใช้เพื่อกิจกรรมบางกิจกรรม ไม่ได้ใช้งานตลอดไป เช่น ใช้เพื่อการประชุม/สัมมนา หรือโครงการระยะสั้น หากผู้ขอใช้ทราบระยะเวลาในการใช้งานที่แน่นอนสามารถขอยกเลิก NetID ดังกล่าวได้หลังสิ้นสุดกิจกรรมเพื่อป้องกันการถูกขโมยบัญชีไปใช้งานทำให้เกิดความเสียหายตามมาได้ โดยมีกระกวนการการดำเนินการ ดังนี้

1) หน่วยงานทำบันทึกแจ้งมายังสำนักเรื่องขอยกเลิก NetID หน่วยงาน หรือ หลักสูตร

2) ผู้ดูแลระบบตรวจสอบข้อมูลในบันทึก หากข้อมูลไม่ถูกต้องครบถ้วนหรือมีข้อสงสัยให้ประสานงานกับทางหน่วยงานที่ขอรับบริการ
3) ตรวจสอบในระบบ AMS ว่ามี NetID ที่แจ้งมาในระบบหรือไม่ หากไม่มี NetID นั้นให้แจ้งหน่วยงานที่ขอรับบริการ
4) บันทึกงานในระบบ MES
5) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
6) เลือก กำหนด Account สำหรับหน่วยงาน หรือ หลักสูตร จากเมนู หน่วยงาน หรือ หลักสูตร แล้วค้นหาชื่อ NetID ที่ต้องการยกเลิก
7) ยกเลิก NetID สำหรับหน่วยงาน หรือ หลักสูตร ในระบบ AMS โดยเลือกบัญชีที่ต้องการยกเลิกและเลือก “ลบ”

ภาพที่ 4-13 : การยกเลิก NetID หน่วยงาน หรือ หลักสูตร

8) เมื่อเลือกลบ NetID แล้ว ระบบจะยังไม่ลบ NetID นั้นแบบถาวร ผู้ดูแลระบบยังสามารถคลิก “สร้าง” เพื่อยกเลิกการลบบัญชีนั้นได้ หากผู้ดูแลระบบต้องการยกเลิก NetID แบบถาวร ให้คลิกที่ ถังขยะ เพื่อยืนยันการลบ NetID

ภาพที่ 4-14 : เลือกสร้างเพื่อยกเลิกการลบ หรือ คลิกที่ถังขยะเพื่อยืนยันการยกเลิก NetID

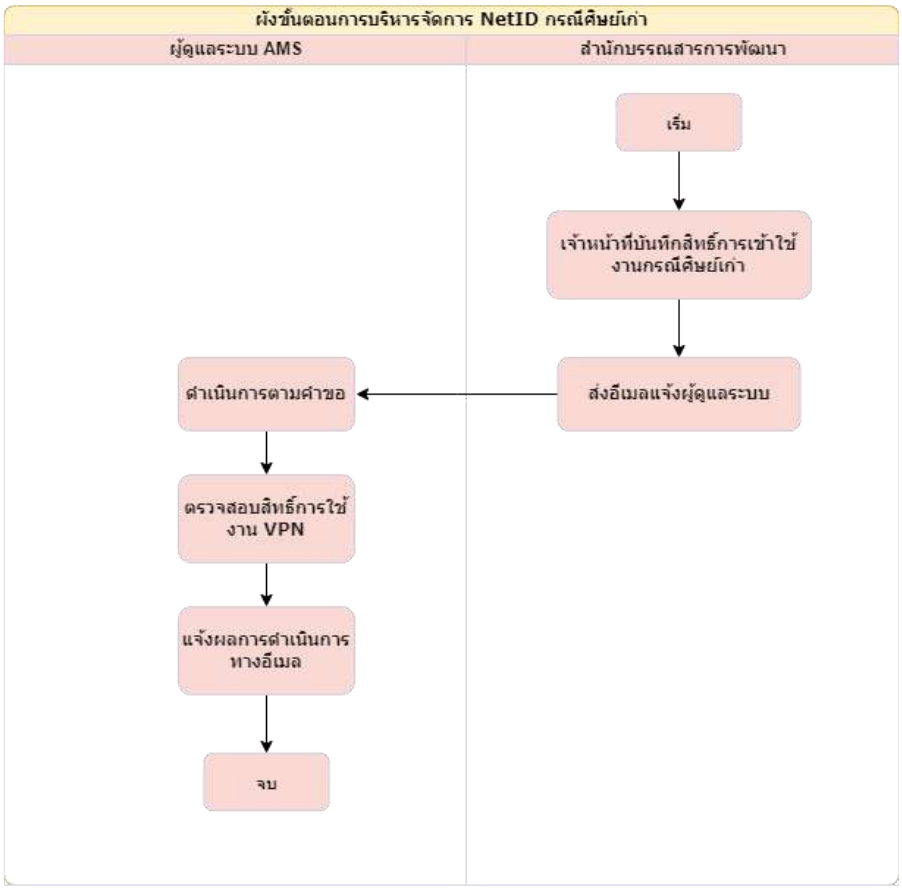
9) ปิดงานในระบบ MES

ข้อสังเกต ข้อควรระวัง : หากยืนยันการลบ NetID นั้นจะถูกลบออกจากระบบ AD และ ระบบ Microsoft 365 อย่างถาวร

4.1.4 การบริหารจัดการ NetID กรณีศิษย์เก่า

การบริหารจัดการ NetID กรณีศิษย์เก่าเป็นการอนุมัติสิทธิ์การใช้งาน VPN (Virtual Private Network) ให้แก่นักศึกษาที่สำเร็จการศึกษาแล้ว เนื่องจากศิษย์เก่าจะไม่สามารถใช้ VPN เพื่อเข้าใช้บริการฐานข้อมูลของห้องสมุดได้ หากศิษย์เก่าประสงค์จะใช้บริการดังกล่าวต้องแจ้งความจำนงไปยังห้องสมุดเพื่อให้ห้องสมุดดำเนินการตามขั้นตอนการให้บริการต่อไป ผู้ดูแลระบบมีหน้าที่บริหารจัดการ NetID กรณีศิษย์เก่าโดยมีผังขั้นตอน และกระบวนการดำเนินการ ดังนี้

ผังขั้นตอนการบริหารจัดการ NetID กรณีศิษย์เก่า



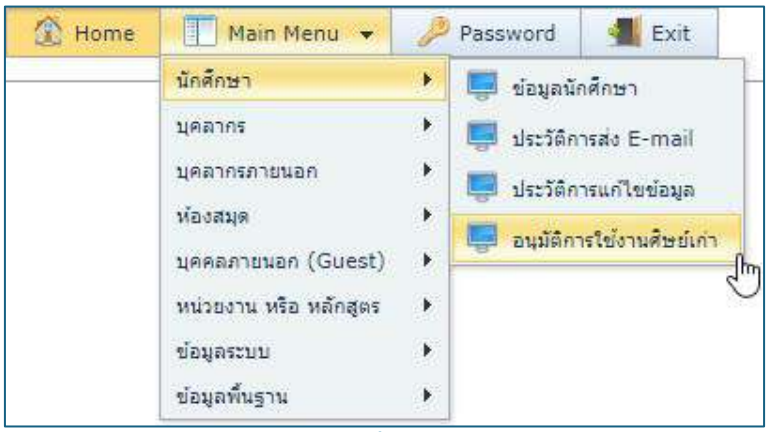
ภาพที่ 4-15 : ผังขั้นตอนการอนุมัติการใช้งานศิษย์เก่า

กระบวนการบริหารจัดการ NetID กรณีศิษย์เก่า

1) เจ้าหน้าที่ห้องสมุดบันทึกสิทธิ์การเข้าใช้งานของศิษย์เก่าในระบบ AMS หลังจากที่บันทึกข้อมูลเสร็จระบบจะส่งอีเมลแจ้งมายังผู้ดูแลระบบ
2) เจ้าหน้าที่ห้องสมุดแจ้งผู้ดูแลระบบทางอีเมลเพื่ออนุมัติสิทธิ์การใช้งาน

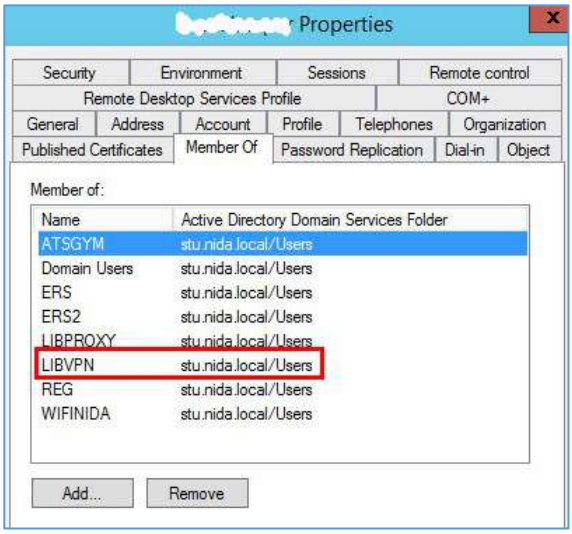
ข้อสังเกต ข้อควรระวัง : การอนุมัติการใช้งานศิษย์เก่าเพื่อให้สิทธิในการใช้บริการ VPN ตามที่ห้องสมุดร้องขอ ระบบ AMS จะตรวจสอบข้อมูลศิษย์เก่าจากระบบทะเบียน และ ทำเนียบศิษย์เก่า ในกรณีศิษย์เก่าที่ไม่มีอีเมลสำรองในระบบ หรือต้องการเปลี่ยนแปลงอีเมลสำรองในระบบสามารถแจ้งห้องสมุดเพื่อดำเนินการบันทึกข้อมูลให้เป็นปัจจุบัน

3) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
4) เลือกเมนู นักศึกษา และเลือก อนุมัติการใช้งานศิษย์เก่า เพื่ออนุมัติ NetID ศิษย์เก่าตามที่เจ้าหน้าที่ห้องสมุดได้บันทึกรายการในระบบ



ภาพที่ 4-16 : การบริหารจัดการ NetID กรณีศิษย์เก่า

5) ตรวจสอบสิทธิการเข้าใช้งาน VPN ที่ AD โดย NetID ศิษย์เก่าที่อนุมัติในระบบจะต้องเป็นสมาชิกกลุ่ม LIBVPN



ภาพที่ 4-17 : ตรวจสอบสิทธ์การใช้งาน NetID กรณีศิษย์เก่าบนระบบ AD

6) แจ้งผลการอนุมัติการใช้งานศิษย์เก่าไปยังห้องสมุดผ่านช่องทางอีเมล

4.2 การบริหารจัดการกลุ่มผู้ใช้งาน และการให้สิทธิ์ระบบที่ให้บริการ

หน้าที่ของผู้ดูแลระบบ AMS นอกจากการบริหารจัดการ NetID แล้วยังมีหน้าที่ดังต่อไปนี้

4.2.1 การบริหารจัดการกลุ่มผู้ใช้งาน

4.2.2 การให้สิทธิ์ระบบที่ให้บริการ

4.2.1 การบริหารจัดการกลุ่มผู้ใช้งาน

ระบบ AMS มีการแบ่งกลุ่มผู้ใช้งาน และกำหนดเมนูการใช้งานระบบตามกลุ่มผู้ใช้งาน ดังนี้

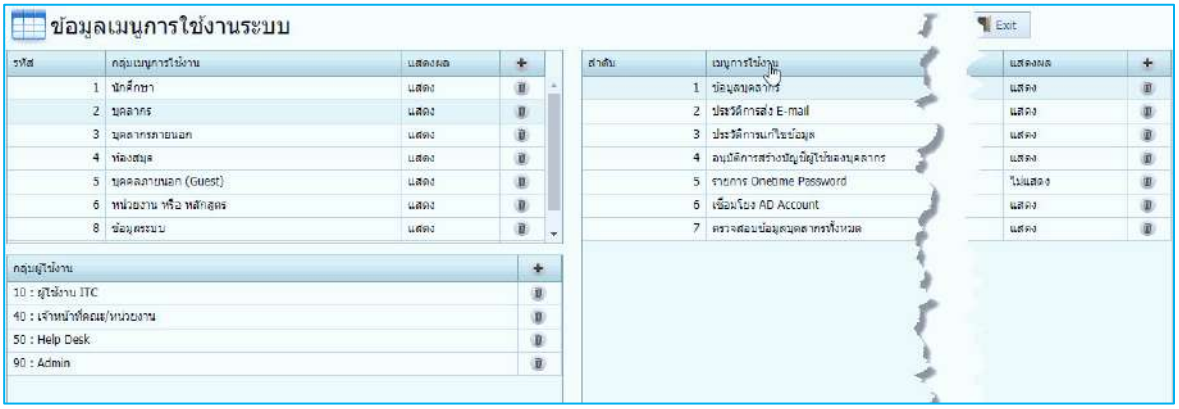
1 **ผู้ใช้งาน ITC** ผู้ใช้งานกลุ่มนี้สามารถดูข้อมูลเบื้องต้นของ NetID บุคลากร นักศึกษา สิทธิ์การใช้งานกรณีศิษย์เก่า

2 **เจ้าหน้าที่คณะ/หน่วยงาน** (ปัจจุบันไม่มีการใช้งานของกลุ่มผู้ใช้งานนี้แล้ว)

3 **Helpdesk** (ปัจจุบันไม่มีการใช้งานของกลุ่มผู้ใช้งานนี้แล้ว)

4 **เจ้าหน้าที่ห้องสมุด** ผู้ใช้งานกลุ่มนี้คือเจ้าหน้าที่ห้องสมุดที่มีหน้าที่ในการบันทึกสิทธิ์การเข้าใช้งานของศิษย์เก่า บันทึก หรือแก้ไขอีเมลสำรองของศิษย์เก่า

5 **Admin** มีสิทธิ์ในการกำหนดค่าต่างๆ เพื่อบริหารจัดการภายใต้ระบบ AMS



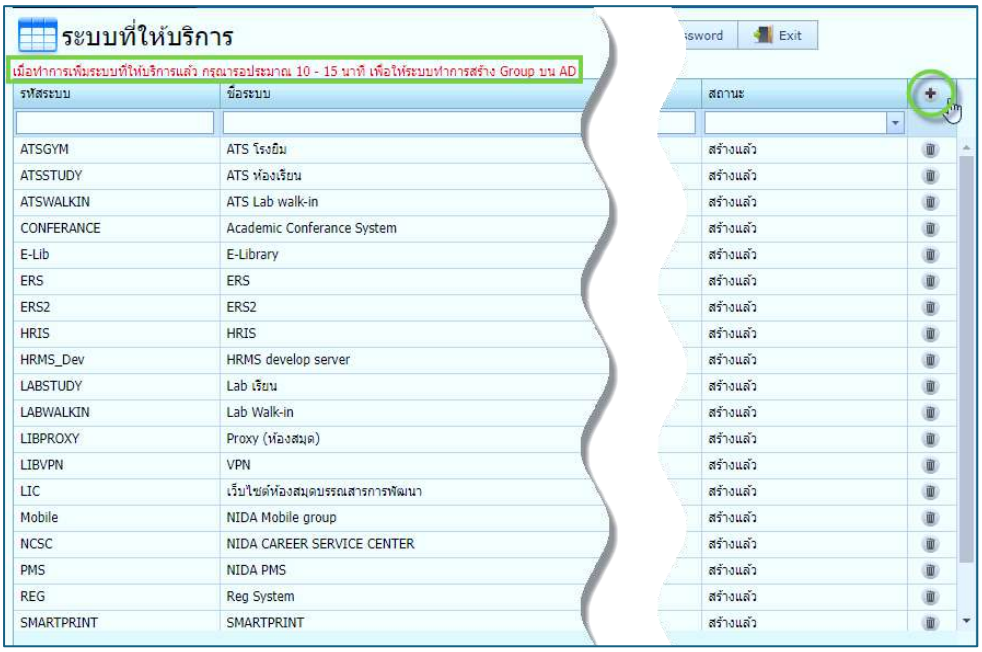
ภาพที่ 4-18 : กลุ่มผู้ใช้งาน และเมนูที่กลุ่มผู้ใช้งานสามารถใช้งานได้

ข้อสังเกต ข้อควรระวัง : ผู้มีสิทธิ์เป็น Admin สามารถบริหารจัดการเมนูให้แสดง หรือไม่แสดงเมนูต่างๆแก่กลุ่มผู้ใช้งานต่างๆได้

4.2.2 การให้สิทธิ์ระบบที่ให้บริการ

การสร้าง NetID ผ่านระบบ AMS จะมีการให้สิทธิ์ระบบที่ให้บริการแก่ NetID ที่สร้างขึ้นโดยมีกลุ่มผู้ใช้งานหลัก 3 กลุ่ม คือ นักศึกษา บุคลากร หน่วยงานหรือหลักสูตร เมื่อมีระบบสารสนเทศใหม่ที่ให้บริการ หรือหากต้องการยกเลิกระบบสารสนเทศที่เคยให้บริการผู้ดูแลระบบต้องดำเนินการดังนี้

1) ผู้ดูแลระบบล็อคอินเข้าระบบ AMS เลือก Main Menu
2) ดำเนินการเพิ่ม/ยกเลิกระบบที่ให้บริการผ่านเมนูข้อมูลระบบ และระบบที่ให้บริการ
3) คลิกที่เครื่องหมาย + เพื่อให้สิทธิ์ระบบที่ต้องการ หรือคลิกที่ ถังขยะ เพื่อยกเลิกระบบที่ต้องการให้สิทธิ์



ภาพที่ 4-19 : การเพิ่มระบบใหม่ หรือยกเลิกระบบที่ให้บริการ

บทที่ 5
ปัญหาอุปสรรคและข้อเสนอแนะ

ผู้ดูแลระบบที่มีหน้าที่ในการบริหารจัดการบัญชีผู้ใช้งานผ่านระบบ AMS ต้องมีความเข้าใจในกระบวนการที่จะได้มาซึ่ง NetID ประเภทต่างๆ รวมทั้ง NetID ประเภทอื่นๆที่นอกเหนือจากการบริหารจัดการผ่านระบบ AMS เนื่องจากความจำเป็นในการใช้งานที่มากขึ้นเพื่อให้สอดคล้องกับนโยบายต่างๆของทางสถาบัน รองรับการให้บริการ และการบริหารงานต่างๆให้ดำเนินไปด้วยความเรียบร้อย อีกทั้งยังต้องประสานงานกับบริษัท หน่วยงานต่างๆ ภายในสถาบัน ร่วมแก้ไขปัญหารวมทั้งให้คำแนะนำผู้ใช้งานอยู่เสมอๆ

5.1 ปัญหาอุปสรรคและแนวทางแก้ไข

จากการปฏิบัติงานการบริหารจัดการ NetID ประเภทต่างๆ มีปัญหาอุปสรรคในการดำเนินการของขั้นตอนต่างๆ ดังนี้

ขั้นตอนการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข
การสร้าง NetID ของนักศึกษา	1) สถาบันมีหลักสูตร/โครงการที่เปิดใหม่ และระบบ AMS ยังไม่รองรับ ทำให้ไม่สามารถสร้าง NetID ให้แก่นักศึกษาได้	1) ปรับปรุงระบบ AMS และระบบ REG ให้สามารถทำงานที่สัมพันธ์กันได้ เมื่อระบบ REG มีการสร้างหลักสูตร/โครงการที่เปิดใหม่ ระบบ AMS ต้องสามารถปรับโครงสร้างให้รองรับกับหลักสูตร/โครงการใหม่ได้โดยอัตโนมัติ
	2) นักศึกษาที่เรียนมากกว่า 1 หลักสูตร/โครงการจะมี NetID มากกว่า 1 บัญชี	2) สถาบันต้องพัฒนาระบบ REG และระบบ AMS ให้รองรับกับแพลตฟอร์มการเรียนรู้แบบใหม่ที่เป็นการเรียนรู้ตลอดชีวิต (Lifelong Learning) โดย 1 คน มี 1 NetID แต่สามารถใช้งานระบบสารสนเทศได้ทุกๆ ระบบ

ขั้นตอนการดำเนินงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข
การสร้าง NetID บุคลากร	บุคลากรใหม่ได้ NetID ล่าช้าเนื่องจากต้องรอกองบริหารทรัพยากรบุคคลบันทึกข้อมูลของบุคลากรใหม่เข้าระบบ	กองบริหารทรัพยากรบุคคลควรมีการพัฒนาระบบให้สามารถดึงข้อมูลบุคลากรที่มีการบันทึกตั้งแต่การรับสมัครสอบเข้าทำงานโดยข้อมูลที่บันทึกต้องเป็นข้อมูลที่ดึงมาจากส่วนกลางของภาครัฐมาเพื่อใช้ในการสร้าง NetID ได้เลย เพื่อป้องกันความผิดพลาดในการคีย์ข้อมูล และเพื่อความสะดวกรวดเร็วในการสร้าง NetID ของบุคลากรใหม่
การยกเลิก NetID ของบุคลากร	ไม่มีการยกเลิก NetID บุคลากรที่ลาออกเนื่องจากผู้ดูแลระบบไม่ได้รับแจ้งข้อมูลการลาออก	กองบริหารทรัพยากรบุคคลควรมีการพัฒนาระบบการแจ้งข้อมูลบุคลากรเมื่อถูกปรับสถานะเป็นลาออก โดยให้ระบบแจ้งข้อมูลมายังผู้ดูแลระบบ AMS เพื่อทำการยกเลิก NetID ของบุคลากรที่ลาออกต่อไป
การเปลี่ยนผู้รับผิดชอบ NetID สำหรับหน่วยงานหรือหลักสูตร	เมื่อบุคลากรที่รับผิดชอบ NetID สำหรับหน่วยงานหรือหลักสูตรลาออก ผู้รับผิดชอบในระบบจะยังไม่ถูกเปลี่ยนจนกว่าหน่วยงานจะมีการแจ้งเปลี่ยนผู้รับผิดชอบมายังสำนัก	ปรับปรุงระบบ AMS เมื่อบุคลากรถูกปรับสถานะเป็น ลาออก ให้ทำการตรวจสอบว่าบุคลากรที่มีสถานะเป็น ลาออก นั้นเป็นผู้รับผิดชอบ NetID สำหรับหน่วยงานหรือหลักสูตรใดหรือไม่ เพื่อผู้ดูแลระบบจะได้ประสานไปยังหน่วยงานเจ้าของ NetID ให้แจ้งเปลี่ยนผู้รับผิดชอบใหม่
การบริหารจัดการ NetID กรณีศิษย์เก่า	Group การใช้งาน LIBVPN บน AD ไม่ถูกกำหนดให้ NetID ที่ได้ต่ออายุการใช้งาน หลังจากได้อนุมัติการใช้งานศิษย์เก่าแล้ว	ปรับปรุงระบบ AMS โดยทุกครั้งที่ดำเนินการต่ออายุการใช้งานกรณีศิษย์ก่าให้ระบบตรวจสอบ Group LIBVPN ของ NetID นั้นบน AD ว่าได้ถูกกำหนดแล้วหรือไม่

ตารางที่ 5-1 : ปัญหาอุปสรรคและข้อเสนอแนะ

5.2 ข้อเสนอแนะ

1. สถาบันควรพัฒนาระบบสารสนเทศหลักให้สามารถทำงานเชื่อมโยงถึงกันได้ทุกระบบ และรองรับการเปลี่ยนแปลงในอนาคต เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้อง และมีประสิทธิภาพยิ่งขึ้น
2. สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ กฎหมายต่างๆที่เกี่ยวข้อง เช่น กฎหมายเกี่ยวกับ PDPA ,พรบ.คอมพิวเตอร์ แก่บุคลากรอย่างสม่ำเสมอ เพื่อป้องกันการกระทำผิดจากความรู้เท่าไม่ถึงการณ์

บรรณานุกรม

นพดล นิ่มหมู. (2565). หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยโดยศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับ พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540. วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม, 41(3), 64-66.

งานทะเบียนและประมวลผลการศึกษา Office of The Registrar, Educational Service Division. (2568). จาก https://reg.nida.ac.th/

ระบบสื่อสารเพื่อสนับสนุนการเรียนการสอน (Account Management System) [Web application software]. จาก https://ams.nida.ac.th/vnadman/

สถาบันบัณฑิตพัฒนบริหารศาสตร์. (2567, 16 มกราคม). ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง การจัดการบริการ Microsoft 365

สถาบันบัณฑิตพัฒนบริหารศาสตร์. (2564, 30 พฤศจิกายน). ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. 2564

สถาบันบัณฑิตพัฒนบริหารศาสตร์. (2552). ข้อบังคับสถาบันบัณฑิตพัฒนบริหารศาสตร์ ว่าด้วยจรรยาบรรณของบุคลากรสถาบัน พ.ศ.2552 หมวด 2

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ. (2568). วิสัยทัศน์ พันธกิจ, จาก https://idt.nida.ac.th/about/vision-mission/

Microsoft. (2568). Microsoft 365 คืออะไร, จาก https://support.microsoft.com/th-th/office/microsoft-365-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3-847caf12-2589-452c-8aca-1c009797678b

sakid. (2565). PDCA คืออะไร รู้จักหลักการที่ทำให้งานของคุณมีประสิทธิภาพยิ่งขึ้น. วันที่ค้นข้อมูล 16 ตุลาคม 2567, จาก https://www.sakid.app/blog/pdca-organization-development/