



บันทึกข้อความ

สำนักเทคโนโลยีดิจิทัลเพื่อการศึกษา
รับที่ 614
วันที่ 18 มิ.ย. 2567
โทร. ๑๔๑๗ 15.1๗ น.

ส่วนราชการ กลุ่มตรวจสอบภายใน สำนักงานเลขาธิการสภาการศึกษา

ที่ ศธ ๐๓๐๘/๕๙ วันที่ ๑๘ มิถุนายน ๒๕๖๗

เรื่อง แจ้งเปิดตรวจการตรวจสอบด้านสารสนเทศ

เรียน ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล

ตามบันทึกข้อความ กลุ่มตรวจสอบภายใน ที่ ศธ ๐๓๐๘/๗๔ ลงวันที่ ๒๙ กันยายน ๒๕๖๖ เลขาธิการสภาการศึกษาอนุมัติแผนการตรวจสอบประจำปีงบประมาณ พ.ศ. ๒๕๖๗ โดยกำหนดให้ตรวจสอบการดำเนินงานด้านสารสนเทศ นั้น

กลุ่มตรวจสอบภายใน ขอแจ้งเปิดตรวจการตรวจสอบดังกล่าว และขอให้ท่านพิจารณาถึงความเหมาะสมของวัตถุประสงค์ ขอบเขตการตรวจสอบ รายละเอียดดังตารางที่แนบมาท้ายหนังสือนี้

จึงเรียนมาเพื่อโปรดพิจารณา หรือหากท่านประสงค์ให้ปรับวัตถุประสงค์และขอบเขตการตรวจสอบ ขอให้แจ้งกลับภายในวันพุธที่ ๒๖ มิถุนายน ๒๕๖๗ โดยกลุ่มตรวจสอบภายในมอบหมายให้ นางสาววิไลรัตน์ พวงพิทักษ์ เป็นผู้ประสานงานกับผู้รับผิดชอบโดยตรง

(นางสาวพัชราภรณ์ ศรีคล้าย)
ผู้อำนวยการกลุ่มตรวจสอบภายใน

มอบแจ้ง

ก.เทคโนโลยี ก.ไซเบอร์

ก.บริหารข้อมูล ผบท.

ทราบและถือปฏิบัติ

ดำเนินการต่อไป

(นายภาณุพงศ์ พนมวัน)

นักวิชาการศึกษานโยบายพิเศษ รักษาราชการแทน
ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลเพื่อการศึกษา

18 มิ.ย. 2567

19/6/67

๗.๖.๖๗

“เรียนดี มีความสุข”

ตรวจสอบ
น.ส.วิไลรัตน์ พวงพิทักษ์
๑๘ มิ.ย. ๖๗

รายละเอียดวัตถุประสงค์และขอบเขตการตรวจสอบ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗
สำนักงานเลขาธิการสภาการศึกษา

หน่วยรับตรวจ / เรื่องที่ตรวจ	วัตถุประสงค์ การตรวจสอบ	ขอบเขตการตรวจสอบ	เอกสาร ประกอบการตรวจสอบ
<p>หน่วยรับตรวจ : สำนักเทคโนโลยี ดิจิทัลเพื่อการศึกษา</p> <p>การตรวจสอบการดำเนินงานด้าน สารสนเทศ</p>	<p>เพื่อสอบถามระบบการควบคุมภายในการปฏิบัติงานด้านสารสนเทศ</p>	<p>๑. ตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)</p> <p>๒. ตรวจสอบการดำเนินการระบบ IT Security</p> <p>๓. ตรวจสอบการดำเนินการระบบ Cyber Security</p>	<p>การสัมภาษณ์การดำเนินงานด้านสารสนเทศ รายละเอียด ตามแบบสอบถามตั้งแบบ</p>

การตรวจสอบการดำเนินงานด้านสารสนเทศ

เรื่องที่ตรวจสอบ : การตรวจสอบการดำเนินงานด้านสารสนเทศ

ประเด็นการตรวจสอบ : การสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

วัตถุประสงค์ : เพื่อสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

ขอบเขตการตรวจสอบ : การตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๑. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเลขาธิการสภาการศึกษา			
๑.๑ การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล สกศ.			
๑.๒ การสำรองข้อมูลของระบบงาน			
๑.๓ การทดสอบระบบสารสนเทศ การทดสอบระบบสำรองข้อมูล การทดสอบการกู้คืนข้อมูล			
๑.๔ การบริหารจัดการคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ			
๒. โครงสร้างทางดานความมั่นคงปลอดภัยของระบบสารสนเทศ			
๒.๑ การมอบหมายเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัย			
๒.๒ ความรู้ความสามารถพื้นฐานของเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัยเพียงพอเหมาะสมต่อการปฏิบัติงาน			
๒.๓ การบริหารจัดการความมั่นคงปลอดภัย เช่น ระบบงานเกิดปัญหา หยุดชะงักไม่สามารถดำเนินการได้อย่างต่อเนื่อง เป็นต้น			
๓. การควบคุมการเข้าถึง			
๓.๑ การกำหนดรหัสผ่านเข้าเครื่องคอมพิวเตอร์			
๓.๒ มีการกำหนดสิทธิ์ผู้ดูแลระบบ ผู้ใช้งานระบบ และการเก็บรักษารหัสผ่าน มีตารางแสดงสิทธิ์การเข้าถึงฐานข้อมูล มีการควบคุมและจำกัดสิทธิ์ รวมทั้งมีการทบทวนสิทธิเข้าถึงของผู้ใช้งานอย่างต่อเนื่องเป็นระยะตามที่กำหนดไว้ รวมทั้งมีการกำหนดรหัสผ่านสำหรับการเข้าถึงข้อมูลที่สำคัญ			

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๔. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร			
๔.๑ มีการบริหารจัดการรักษาความปลอดภัยทางกายภาพ และควบคุมพื้นที่การเข้า-ออกพื้นที่ควบคุม ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์			
๕. ความปลอดภัยในการปฏิบัติงาน			
๕.๑ การติดตั้งระบบรักษาความปลอดภัย (เช่น การตรวจจับการแจ้งเตือนการบุกรุก, โปรแกรมสแกนไวรัสคอมพิวเตอร์ เป็นต้น)			
๕.๒ การบันทึก log			
๖. การควบคุมการพัฒนาและการบำรุงรักษาระบบสารสนเทศ			
๖.๑ มีการวางแผนการพัฒนาระบบ			

การตรวจสอบการดำเนินงานด้านสารสนเทศ

เรื่องที่ตรวจสอบ : การตรวจสอบการดำเนินงานด้านสารสนเทศ

ประเด็นการตรวจสอบ : การสอบทานการดำเนินการตามระบบ IT Security

วัตถุประสงค์ : เพื่อสอบทานการดำเนินการตามระบบ IT Security ว่ามีความเหมาะสมเพียงพอ

ขอบเขตการตรวจสอบ : การตรวจสอบการดำเนินการตามระบบ IT Security

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๑. การรักษาความปลอดภัยเครือข่าย (Network Security)			
๑.๑ การกำหนดหน้าที่ความรับผิดชอบ			
๑.๒ การเชื่อมต่อเครือข่าย			
๑.๓ มีการกำหนดชั้นความลับของข้อมูล			
๑.๔ การดูแลเส้นทางของอุปกรณ์เครือข่าย			
๑.๕ การเชื่อมต่อเครือข่าย			
๑.๖ การตรวจจับและการป้องกันการบุกรุก			
๑.๗ แผนผังระบบเครือข่าย			
๑.๘ การบันทึกการทำงานของระบบป้องกันการบุกรุก			
๒. การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security)			
๒.๑ การเข้าสู่ระบบเครือข่ายภายใน สกศ.			
๒.๒ การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ของอุปกรณ์เครือข่าย			
๓. การรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security)			
๓.๑ การยืนยันตัวตนในการใช้งานระบบ			
๓.๒ การจัดการกับมัลแวร์หรือการโจมตีของไวรัส			
๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๔.๑ การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๕. การรักษาความปลอดภัยการใช้งาน			
๕.๑ การใช้งานแอปพลิเคชัน			
๕.๒ Application Security)			

การตรวจสอบการดำเนินงานด้านสารสนเทศ

เรื่องที่ตรวจสอบ : การตรวจสอบการดำเนินงานด้านสารสนเทศ

ประเด็นการตรวจสอบ : การสอบทานการดำเนินการตามระบบ Cyber Security

วัตถุประสงค์ : เพื่อสอบทานการดำเนินการตามระบบ Cyber Security ว่ามีความเหมาะสม เพียงพอ

ขอบเขตการตรวจสอบ : การตรวจสอบการดำเนินการตามระบบ Cyber Security

รายละเอียด	ผลการตรวจสอบ		
	มี	ไม่มี	เอกสารอ้างอิง
๑. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์			
๒. มีการสำรองข้อมูลเป็นประจำทุกวัน และเก็บข้อมูลสำรองไว้มากกว่า ๑ สถานที่			
๓. ดำเนินการตรวจสอบการทำงานของเครื่องแม่ข่ายเป็นประจำ รวมทั้งตรวจสอบช่องโหว่ของระบบ เพื่อตรวจสอบและแก้ไขช่องโหว่ที่อาจส่งผลให้ผู้ไม่หวังดีโจมตีระบบ			
๔. มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล (Cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ			
๕. มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท (Network and Communication Security) โดยมีการป้องกันข้อมูลที่มีการรับส่งผ่านเครือข่ายให้มีความปลอดภัย สามารถป้องกันและเฝ้าระวังการถูกบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้นได้			
๖. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของแม่ข่ายระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไขหรือทำลาย รวมถึงมีการสอบทาน log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ			
๗. ใช้ระบบการสื่อสารแบบรวมศูนย์ (workD Platform)			
๘. ใช้บริการพื้นที่คลาวด์ของภาครัฐ ทั้ง G-Cloud (GDCC) และ MOE Cloud			