แผนบริหารจัดการความเสี่ยง เทคโนโลยีสารสนเทศและการสื่อสาร

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

แผนบริหารจัดการความเสี่ยง
เทคโนโลยีสารสนเทศและการสื่อสาร
กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

สารบัญ

บทนำ

สารบัญ **หน้า**

บทนำ

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสาร กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้บรรลุผลตามวัตถุประสงค์ของหน่วยงาน เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม หน่วยงานจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้น ให้อยู่ในระดับที่หน่วยงานสามารถรองรับได้ ทำให้การปฏิบัติงานมีความมั่นคงปลอดภัยและมีประสิทธิภาพมากยิ่งขึ้น กลุ่มพัฒนาเทคโนโลยีดิจิทัล กองขับเคลื่อนการลดก๊าซเรือกระจก หวังเป็นอย่างยิ่งว่าแผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศ กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมนี้ จะช่วยลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ต่อไป

กลุ่มพัฒนาเทคโนโลยีดิจิทัล
กองขับเคลื่อนการลดก๊าซเรือนกระจก

หลักการและเหตุผล

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของหน่วยงาน

การบริหารจัดการความเสี่ยง จึงมีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ของหน่วยงาน และยังรวมถึงการปกป้องงานตามภารกิจของหน่วยงาน ให้รอดพ้นจากความเสี่ยงที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ซึ่งขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วยงาน ซึ่งมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม เป็นผู้บังคับบัญชาและผู้ดูแลระบบของหน่วยงาน มีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงและเพื่อให้การดำเนินตามภารกิจของหน่วยงานบรรลุผลตามวัตถุประสงค์

วัตถุประสงค์

1. เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในหน่วยงานของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมมีประสิทธิภาพ และปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของกรม

2. เพื่อให้มีการวางแผน กำหนดมาตรการควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม

3. เพื่อเป็นแนวทางการดำเนินการ การกำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ภายในกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

ผลที่คาดว่าจะได้รับ

เพื่อช่วยเพิ่มประสิทธิภาพในการบริหารจัดการ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่อาจมีผลกระทบต่อการปฏิบัติงาน และการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมแล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานตามแผน

ความหมายของการบริหารความเสี่ยง

“ความเสี่ยง (Risk)” หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศของกรมฯ เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไข ซึ่งอาจทำให้กรมฯ เสียชื่อเสียง

“ระดับความเสี่ยงที่ยอมรับได้ (Risk appetite หรือ Acceptable level of risk)” หมายถึง ค่าความเสี่ยงที่หากการประเมินเหตุการณ์ความเสี่ยงหนึ่ง มีค่าน้อยกว่าหรือเท่ากับค่าที่ยอมรับได้นี้ จะถือว่าสินทรัพย์สารสนเทศที่เกี่ยวข้องกับเหตุการณ์ฯ มีความมั่นคงปลอดภัยเพียงพอ และผู้ประเมินความเสี่ยงไม่จำเป็นต้องนำเสนอแผนการลดความเสี่ยงใดๆ เพิ่มเติม

“แผนการลดความเสี่ยง (Treatment plan)” หมายถึง แผนการจัดการกับเหตุการณ์ความเสี่ยงสำหรับกรณีที่ผู้ประเมินความเสี่ยงได้ประเมินเหตุการณ์ความเสี่ยงหนึ่งและพบว่ามีความเสี่ยงเกินกว่าระดับความเสี่ยงที่ยอมรับได้ ผู้ประเมินความเสี่ยงจะต้องนำเสนอแผนการจัดการดังกล่าวต่อหัวหน้างานหรือผู้บังคับบัญชาเพื่อพิจารณาอนุมัติการดำเนินการ

“ปัจจัยเสี่ยง (Risk Factor)” หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใดและจะเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการควบคุมความเสี่ยงในภายหลังได้อย่างถูกต้อง

ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในความรับผิดชอบของกองขับเคลื่อนการลดก๊าซเรือนกระจก กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

สถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการในปัจจุบันของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

ระบบเครือข่ายคอมพิวเตอร์

ระบบเครือข่ายของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (Wire Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองแยกการบริหารจัดการออกจากกัน โดยเครือข่ายใช้สาย (Wire Network) กองขับเคลื่อนการลดก๊าซเรือนกระจกจะเป็นผู้บริหารจัดการ ส่วนระบบเครือข่ายไร้สาย (Wireless Network) จะเป็นการใช้บริการจากผู้ให้บริการอินเตอร์เน็ต (Internet service provider: ISP) โดยมีรายละเอียดของระบบเครือข่ายทั้ง 2 ประเภทดังต่อไปนี้

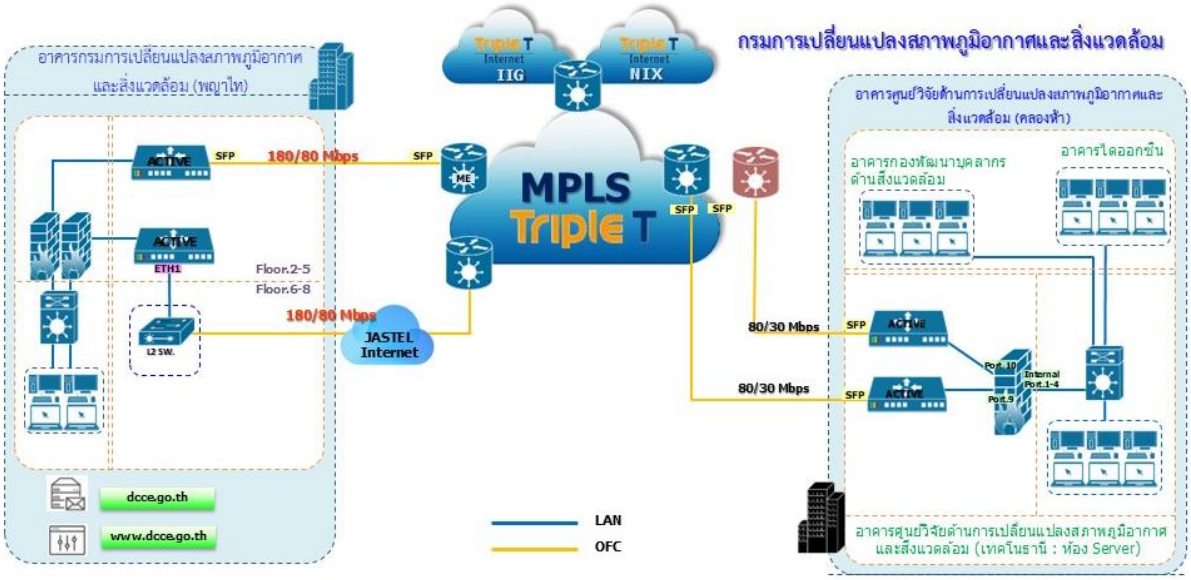
1. ระบบเครือข่ายใช้สาย (Wire Network) กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมมีระบบเครือข่ายใช้สายเชื่อมโยงกันระหว่างที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมและที่

ศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ซึ่งทั้ง 2 สถานที่ ใช้ผู้ให้บริการอินเตอร์เน็ตรายเดียวกันในการเชื่อมโยงระบบเครือข่ายใช้สายเข้าด้วยกันและใช้ในการออกสู่อินเตอร์เน็ต

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม มีโครงข่ายอินเตอร์เน็ต ให้บริการแก่เจ้าหน้าที่ประกอบด้วย

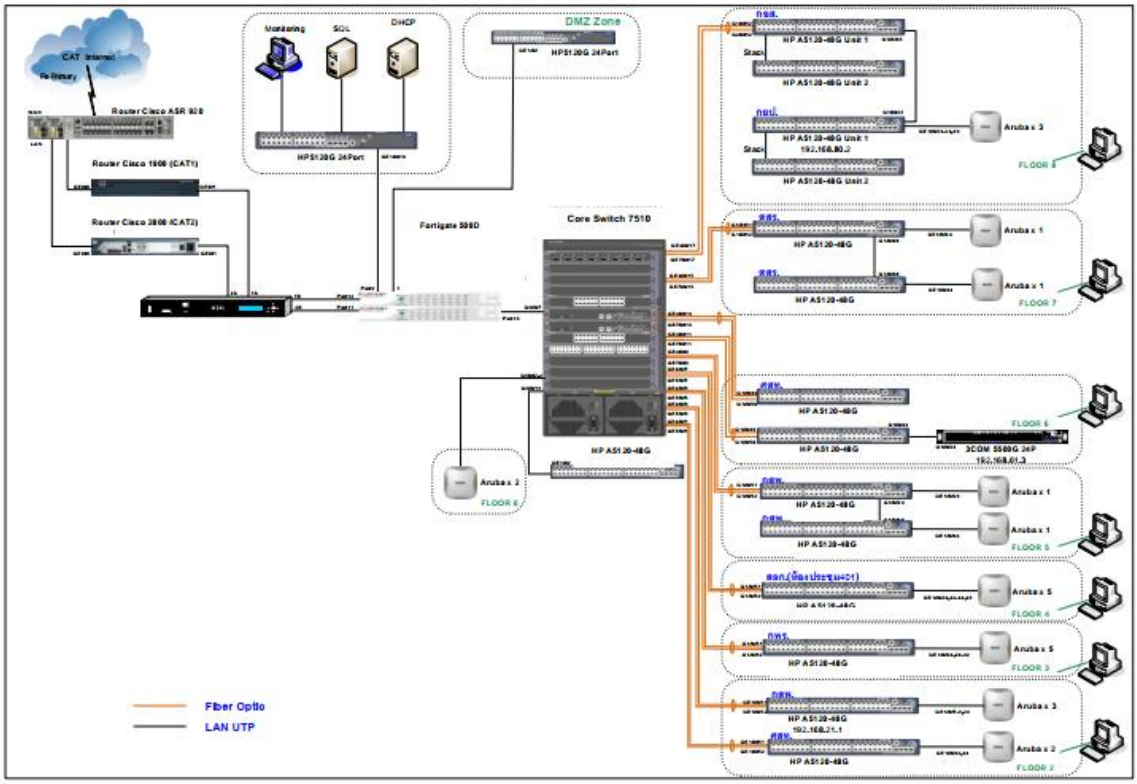
1. เครือข่ายกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ความเร็ว 180/80 Mbps จำนวน 2 โครงข่าย

2. เครือข่ายอาคารศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ความเร็ว 80/30 Mbps จำนวน 2 โครงข่าย



รูปที่ 1 แสดงการเชื่อมโยงระบบเครือข่ายอินเตอร์เน็ต

โดยระบบเครือข่ายใช้สายภายในกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม จะทำการเชื่อมโยงระบบเครือข่ายเข้ากับอุปกรณ์เครือข่ายของผู้ให้บริการอินเตอร์เน็ต (Internet Service provider : ISP) และเชื่อมต่อมายังอุปกรณ์รักษาความมั่นคงปลอดภัยในระบบเครือข่ายของกรมฯ จากนั้น จะทำการต่อเข้ากับอุปกรณ์เครือข่ายหลัก (Core Switch) ก่อนจะทำการกระจายไปยัง สำนัก/กอง/ศูนย์ ตามชั้นต่าง ๆ ตั้งแต่ชั้นที่ 2 ถึงชั้นที่ 8 เพื่อใช้ในการดำเนินงานของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม



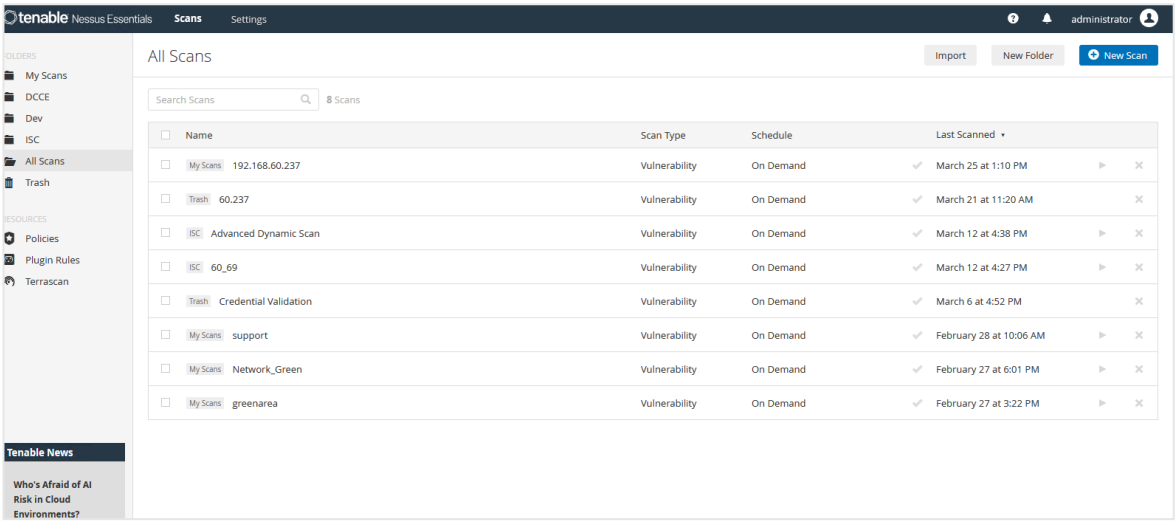
รูปที่ 2 แสดงระบบเครือข่ายที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

กองขับเคลื่อนการลดก๊าซเรือนกระจก ได้ดำเนินการติดตั้งระบบตรวจหาช่องโหว่ในระบบเครือข่ายและไอที (Nesses) ระบบนี้ใช้หลักการและอัลกอริทึมขั้นสูงในการค้นหาจุดอ่อนด้านความปลอดภัยในระบบคอมพิวเตอร์ สามารถตรวจพบช่องโหว่ด้านรหัสโปรแกรมและการตั้งค่าระบบไอทีต่างๆ เพื่อปรับปรุงให้มั่นคงยิ่งขึ้น ดังนี้

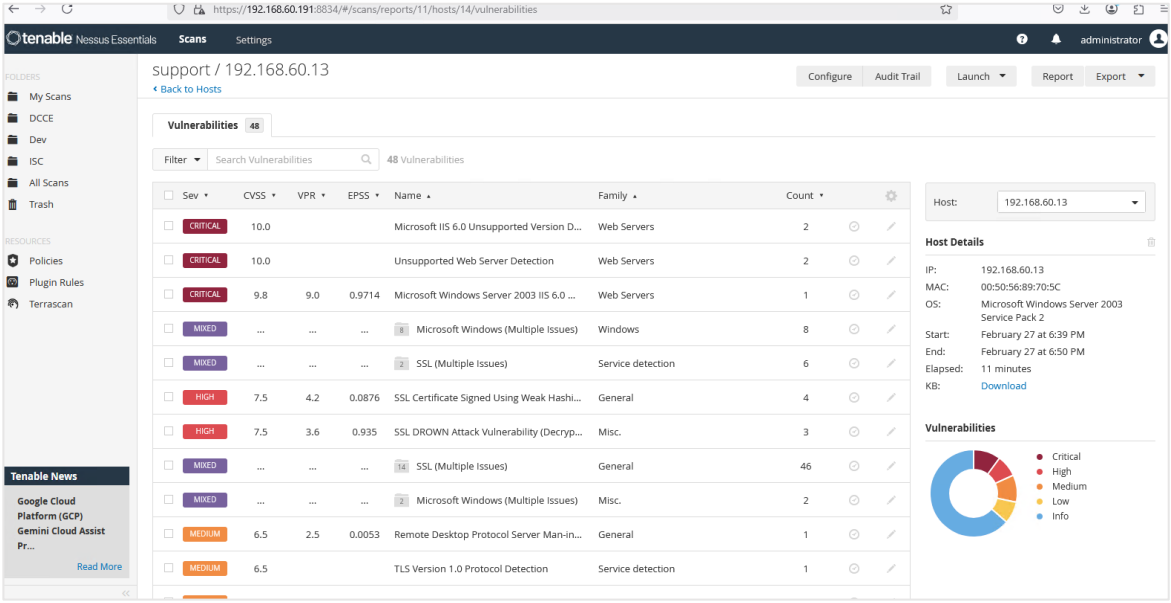
1. **แสดงรายละเอียดของช่องโหว่** จะแสดงรายละเอียดของช่องโหว่ที่พบ รวมถึงระดับความรุนแรงและผลกระทบ ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์และจัดลำดับความสำคัญของการแก้ไข

2. ประสานงานและดำเนินการแก้ไข ประสานงานกับทีมงานเทคนิคเพื่อวางแผนและดำเนินการปิดช่องโหว่อย่างเป็นขั้นตอน เพื่อเพิ่มระดับความปลอดภัยระบบไอทีโดยรวม

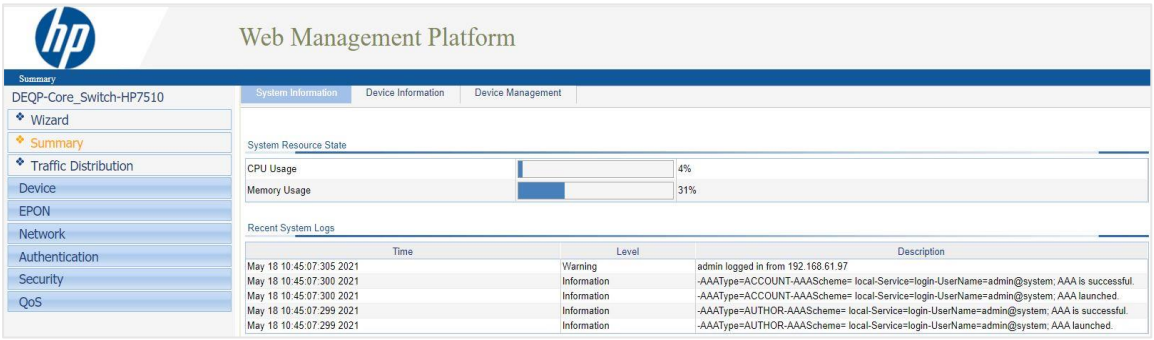
3. จัดทำรายงานการตรวจสอบ จัดทำรายงานการตรวจสอบแบบละเอียด ครอบคลุมข้อมูลเกี่ยวกับช่องโหว่ที่พบ ผลกระทบ และแนวทางการแก้ไข เพื่อนำเสนอต่อผู้บริหาร



รูปที่ 3 แสดงรายการที่ตรวจพบช่องโหว



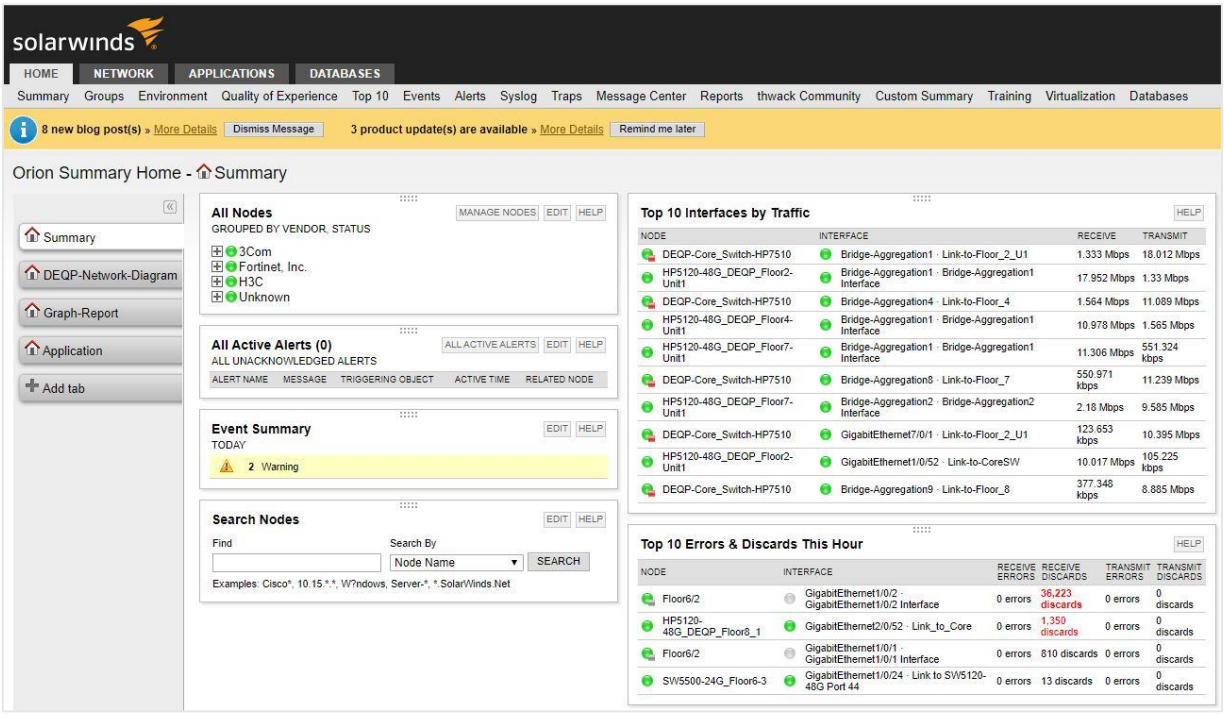
รูปที่ 4 แสดงรายละเอียดของช่องโหว่



รูปที่ 5 แสดงสถานะการทำงานของอุปกรณ์เครือข่ายหลัก (Core Switch)

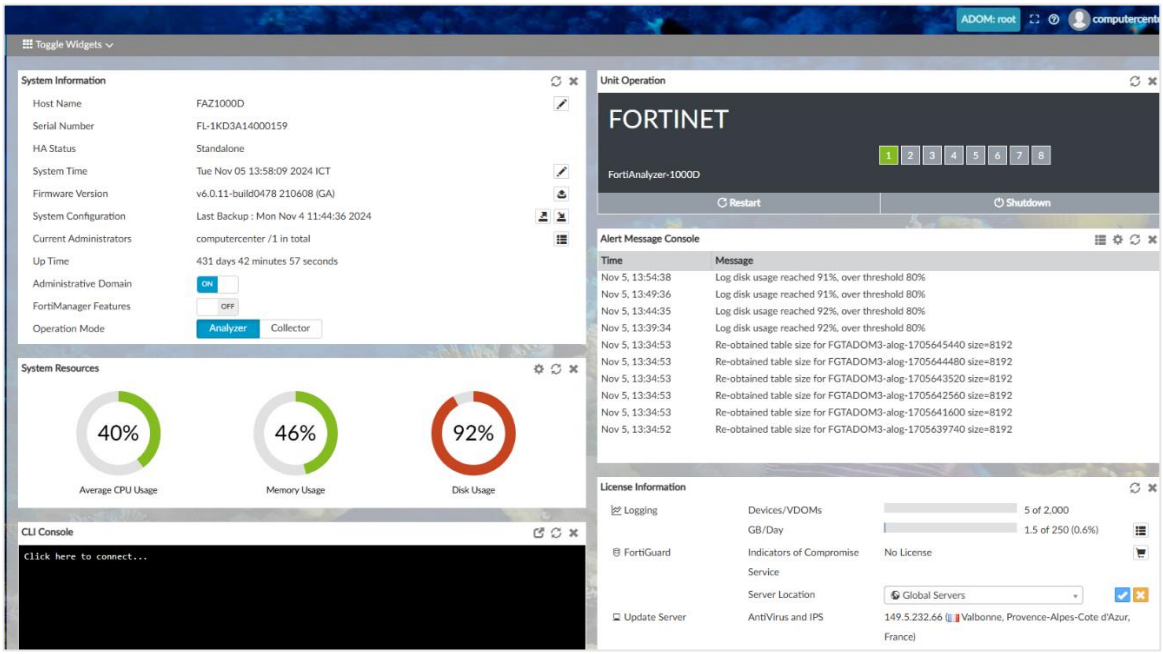
จากรูปที่ 5 แสดงสถานะการทำงานของอุปกรณ์เครือข่ายหลัก (Core Switch) แสดงให้เห็นว่าทรัพยากรเพียงพอต่อการทำงาน โดยจากรูปหน่วยความจำของอุปกรณ์เครือข่ายหลัก ถูกใช้งานร้อยละ 31 และหน่วยประมวลผลถูกใช้งานร้อยละ 4 ส่วนอุปกรณ์เครือข่ายปลายทางตามพื้นที่ต่างๆ ที่ติดตั้งให้กับสำนัก/ศูนย์/กอง มีทรัพยากรเพียงพอต่อการทำงานของอุปกรณ์ รวมทั้งได้รับการดูแล บำรุงรักษา และ แก้ไขปัญหาเช่นเดียวกับอุปกรณ์เครือข่ายหลัก

กองขับเคลื่อนการลดก๊าซเรือนกระจก ได้ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์และระบบเครือข่าย (Solar Wind Network Monitoring) สำหรับใช้ในการติดตามการทำงานของระบบใช้สายของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม



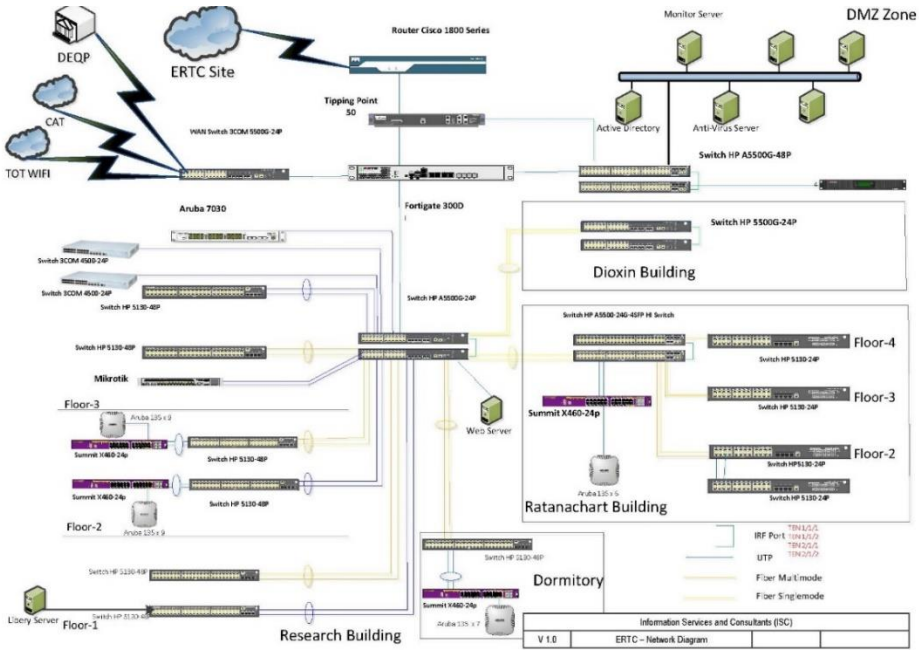
รูปที่ 6 แสดงการทำงานของโปรแกรมติดตามการทำงานของระบบเครือข่าย

พร้อมทั้งติดตั้งระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในเครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยและการดูแลระบบเครือข่ายของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมให้ดียิ่งขึ้น



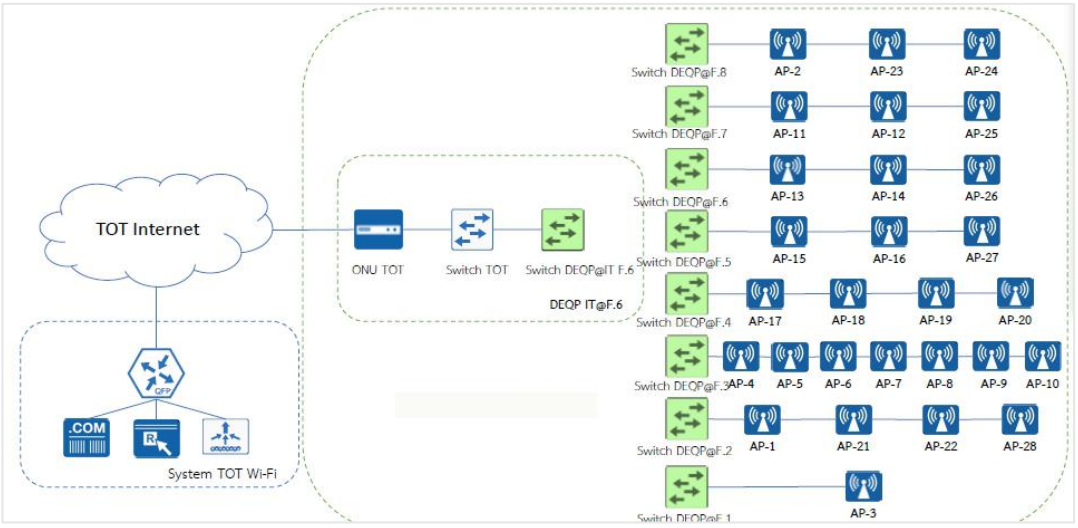
รูปที่ 7 แสดงการทำงานของอุปกรณ์เก็บข้อมูลการจราจรทางอินเตอร์เน็ต

ระบบเครือข่ายใช้สายภายในศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม จะมีลักษณะคล้ายคลึงกันกับที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม คือจะทำการเชื่อมต่อระบบเครือข่ายจากผู้ให้บริการอินเตอร์เน็ตมายังอุปกรณ์ควบคุมเส้นทางในระบบเครือข่ายของศูนย์ฯ (Router) และเชื่อมต่อไปยังอุปกรณ์ป้องกันการบุกรุก (Firewall) แล้วต่อเข้าอุปกรณ์เครือข่ายหลักของศูนย์ฯ (Core Switch) ก่อนจะกระจายไปยังส่วนงานต่างๆ ภายในศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

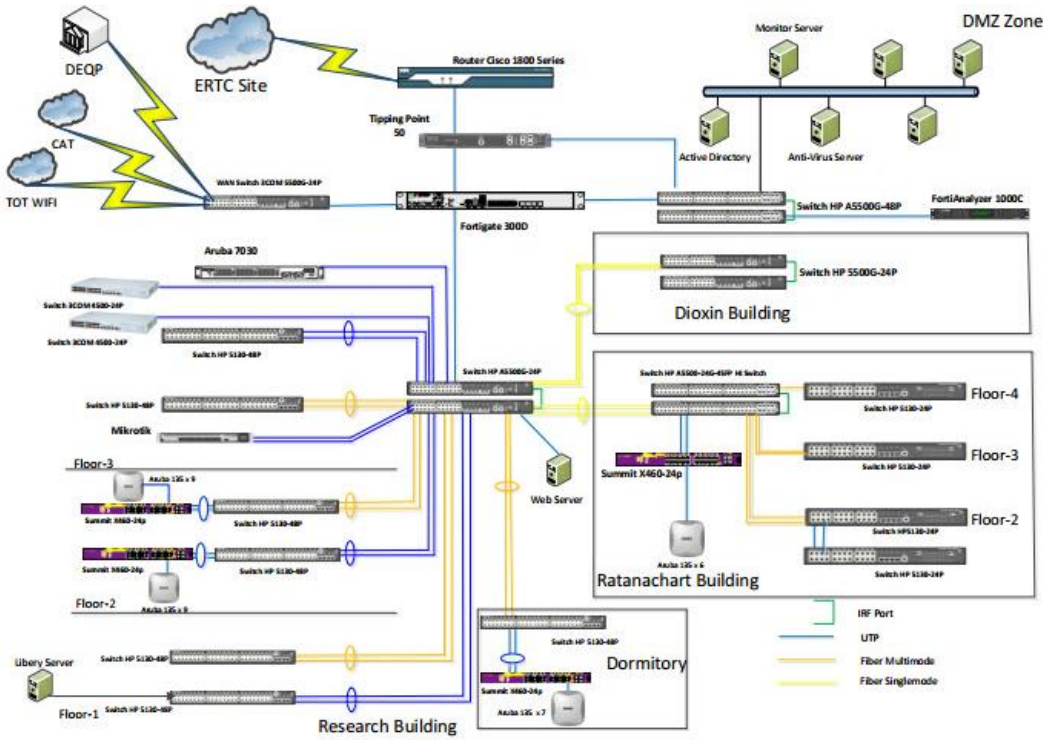


รูปที่ 8 แสดงระบบเครือข่ายที่ศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

2. ระบบเครือข่ายไร้สาย (Wireless Network) ปัจจุบันกรมฯ ได้ใช้บริการระบบเครือข่ายไร้สายจากผู้ให้บริการอินเตอร์เน็ต ทั้งที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมและที่ศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม โดยผู้ให้บริการอินเตอร์เน็ตได้ทำการติดตั้งจุดกระจายสัญญาณ (Access Point) เข้ากับระบบเครือข่ายหลักของกรมฯ และใช้วิธีทางเทคนิคในการบังคับให้ผู้ใช้งานสามารถใช้งานเครือข่ายไร้สายเฉพาะบริการอินเตอร์เน็ตเพียงอย่างเดียว ไม่สามารถเข้าใช้งานระบบงานภายในของกรมฯ ได้ และมีการควบคุมสิทธิในการใช้งานระบบเครือข่ายไร้สายอีกด้วย



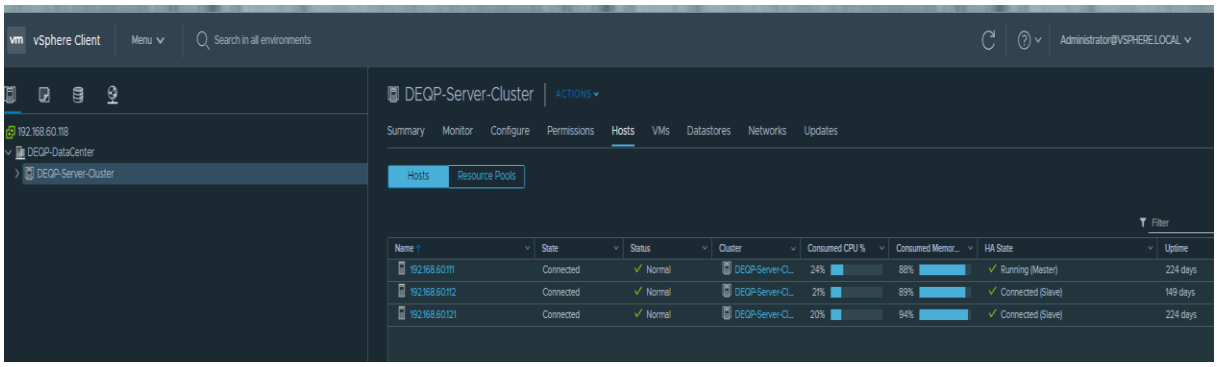
รูปที่ 9 แสดงระบบเครือข่ายไร้สายที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม



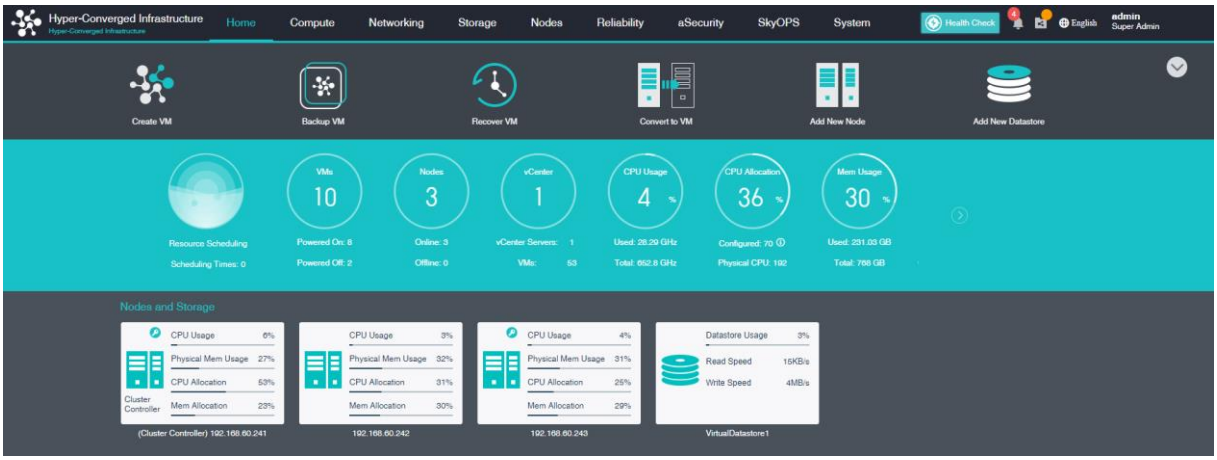
รูปที่ 10 แสดงระบบเครือข่ายไร้สายที่ศูนย์วิจัยการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

ระบบคอมพิวเตอร์

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อมได้ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง ปัจจุบันได้นำเทคโนโลยีเบลดเซิร์ฟเวอร์ (Blade Server) เข้ามาใช้งาน โดยนำเครื่องแม่ข่ายที่มีความสำคัญต่างๆ ไปติดตั้งไว้ในเบลดเซิร์ฟเวอร์ (Blade Server) ซึ่งจะทำให้ลดปัญหาที่เกิดจากอุปกรณ์เครื่องแม่ข่ายชำรุดและส่งผลต่อการหยุดให้บริการของเครื่องแม่ข่ายนั้นได้ โดยระบบที่สำคัญต่อการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่อยู่ในเบลดเซิร์ฟเวอร์ (Blade Server) เช่น ระบบป้องกันไวรัส ระบบติดตามและบริหารการทำงานของระบบเครือข่าย (Network Monitor) ระบบบริหารเครื่องแม่ข่ายเสมือนในเบลดเซิร์ฟเวอร์ และระบบฐานข้อมูลของกรมฯ เป็นต้น

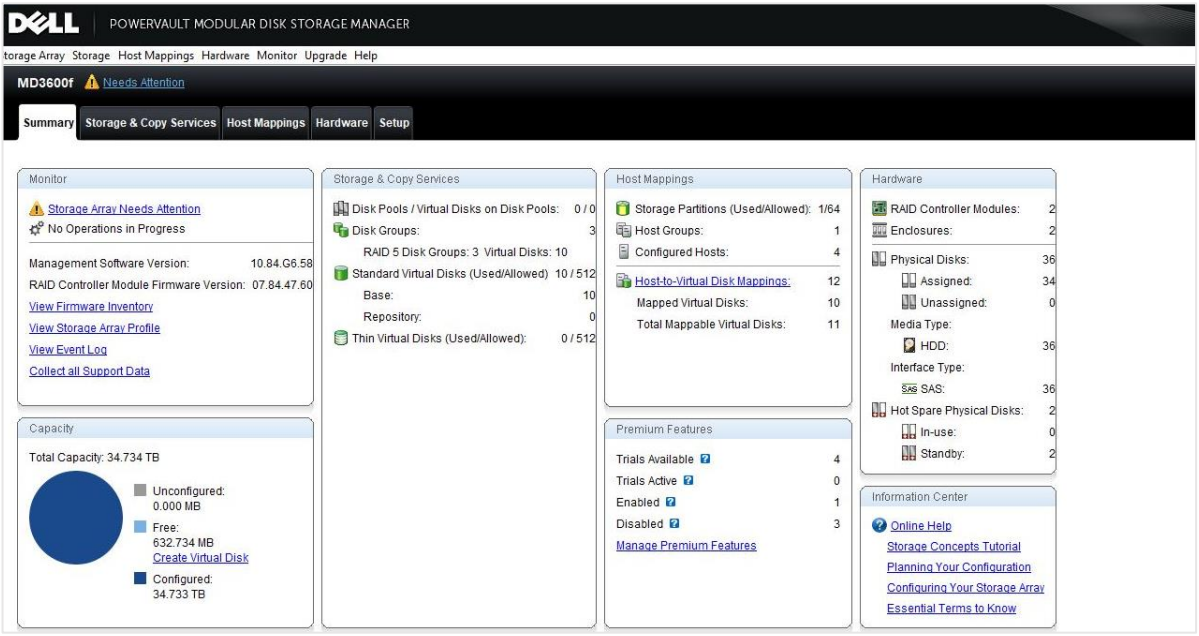


รูปที่ 11 แสดงภาพรวม เบลดเซิร์ฟเวอร์ (Blade Server) ของกรมฯ

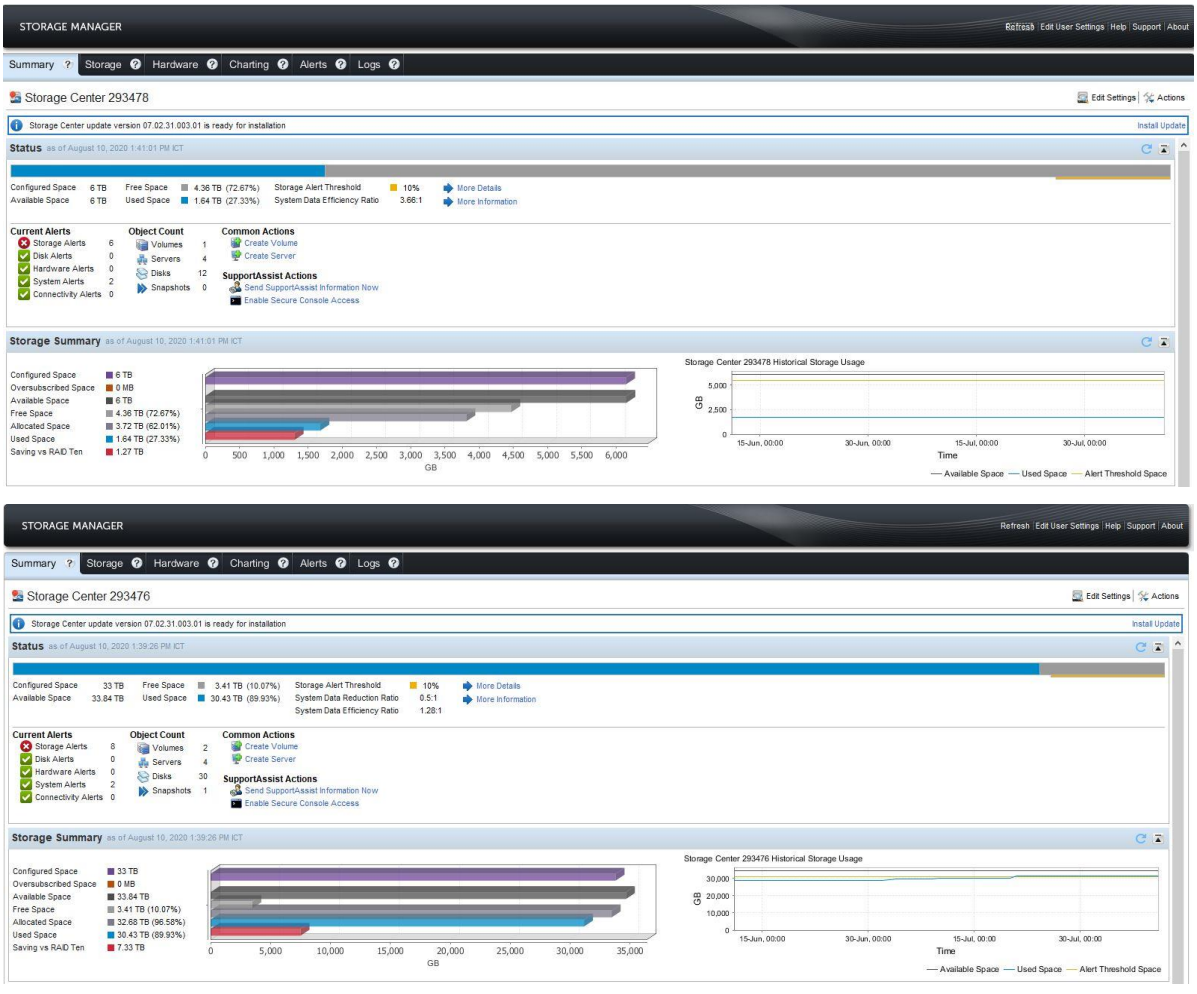


รูปที่ 12 แสดงภาพรวม เบลดเซิร์ฟเวอร์ (Blade Server) ของกรมฯ

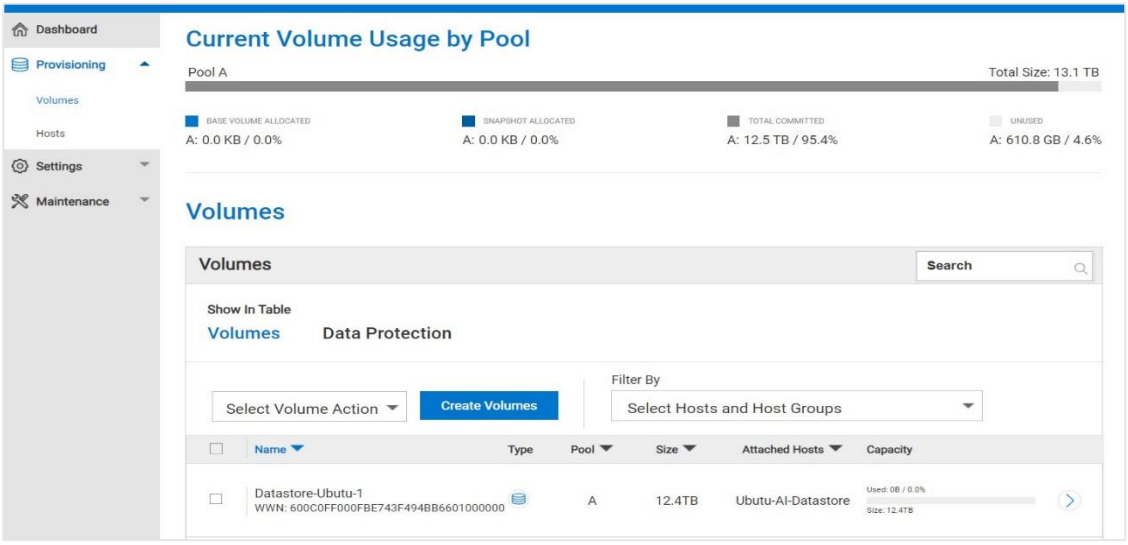
กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม มีระบบบันทึกข้อมูล (Storage) สำหรับจัดเก็บฐานข้อมูล และข้อมูลต่างๆ ของกรมฯ แยกจากเบลดเซิร์ฟเวอร์ (Blade Server) ซึ่งเป็นไปตามหลักการใช้งานเทคโนโลยีนี้ โดยระบบบันทึกข้อมูลมีความจุ (Capacity) ทั้งสิ้นประมาณ 98.68 เทระไบต์ (Tera Byte) ปัจจุบัน มีเนื้อที่เหลือประมาณ 14.04 TB (Tera Byte) หรือประมาณ 14.28 เปอร์เซ็นต์ ของความจุทั้งหมด



รูปที่ 13 แสดงภาพรวมระบบบันทึกข้อมูล (Storage) ของกรมฯ (รุ่น Dell MD3600F)



รูปที่ 14 แสดงระบบบันทึกข้อมูล (Storage) ของกรมฯ (รุ่น PowerVault MD1400)



รูปที่ 15 แสดงระบบบันทึกข้อมูล (Storage) ของกรมฯ (รุ่น SAN_ME5024_AI_Server)

ตารางแสดงเซิฟเวอร์ (Blade Server) ที่อยู่ในความดูแลของกองขับเคลื่อนการลดก๊าซเรือนกระจก

NO.	SERVER	URL	DIVISION	CONTACT	
1	ระบบฐานข้อมูลโครงการมหิงสาสายสืบและมหิงสาสายสืบปฐมวัย	mahingsa.dcce.go.th	กปอ.	จุฑา กีฬา	1528
2	ระบบฐานข้อมูล Eco-School	ecoschool.dcce.go.th	กปอ.	วรรณางค์ พรรณาไพร	1523
3	ระบบฐานข้อมูล Eco-School (เครื่องพัฒนา)	https://devecoschool.dcce.go.th	กปอ.	วรรณางค์ พรรณาไพร	1523
4	CAR - Carbon Awareness and Reduction	carapp.dcce.go.th	กปอ.	วรกร แต้นำชัย	1841
5	T-PLAT INFO	thailandadaptationinfo.dcce.go.th	กปอ.	มนพิสุทธิ์ แก้วศรี	1558
6	actionforclimate-ebook	https://actionforclimate-ebook.dcce.go.th/	กยป.	พีรพงษ์ สุนทรเดชะ	1844
7	ActionforClimate	actionforclimate.dcce.go.th/	กยป.	พีรพงษ์ สุนทรเดชะ	1844
8	ระบบบริหารจัดการและบริการสารสนเทศด้านขยะมูลฝอย โดยกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม	datatrash.dcce.go.th	กลก.	ชานน สวัสดิสวนีย์	1620
9	ระบบ eservice	eservice.dcce.go.th	กลก.	จิรพรรณ เมืองปลื้ม	1623
10	ห้องสมุดกรีนดิจิทัล	greendigitallibrary.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
11	ห้องสมุดอัตโนมัติ	liberty.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
12	ระบบ petition	petition.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620

NO.	SERVER	URL	DIVISION	CONTACT	
13	ระบบจัดเก็บเอกสารจ้างเหมาบุคลากรช่วยปฏิบัติการ	https://300doc.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
14	โครงการแพลตฟอร์มกลางกรีนดิจิทัล ปีงบประมาณ 2566	aigreen.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
15	One Account_Authen	authen.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
16	ระบบคลาวด์ภายในของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม	https://cloud.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
17	ระบบครุภัณฑ์คอมพิวเตอร์ภายในของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม	http://computer.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
18	ระบบฐานข้อมูลผู้ใช้งานกลางของกรมฯ	https://datacenter.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
19	ระบบฐานข้อมูลผู้ใช้งานกลางของกรมฯ	https://datacenter2.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
20	ระบบฐานข้อมูลผู้ใช้งานกลางของกรมฯ	https://datacenter3.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
21	เว็บไซต์กรมฯ	www.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
22	ระบบบัญชีข้อมูล (Data Catalog)	dgf.dcce.go.th	กลก.	โชคดี มั่นคง	1632
23	ระบบจัดเก็บข้อมูลพลังงานและของเสีย	energyandwast.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
24	ระบบจัดเก็บข้อมูลการตรวจวัดคุณภาพสิ่งแวดล้อม	monitor.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
25	ระบบประเมินเมืองสิ่งแวดล้อมยั่งยืน	https://sar.dcce.go.th/	กลก.	ไพลิน พันธุ์แน่น	1633
26	ระบบประเมินเมืองสิ่งแวดล้อมยั่งยืน (เครื่องจัดเก็บเอกสาร)	sarmedia.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
27	ระบบแจ้งซ่อมและติดตามผลครุภัณฑ์คอมพิวเตอร์	support.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
28	เว็บไซต์การจัดงานประชุม TCAC ปี 2565	tcac.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
29	แผนที่ก๊าซเรือนกระจก	tgeis.dcce.go.th	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
30	ระบบประเมินเมืองสิ่งแวดล้อมยั่งยืน (เครื่อง MongoDB)	sar.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
31	ศูนย์การเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม	https://ccecenter.dcce.go.th/	กลก.	สุพรรณี สุวรรณชาติ	1620
32	TGEIS_DB	TGEIS_DB	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
33	gcf	gcf.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
34	กองประสานการจัดการการเปลี่ยนแปลงสภาพภูมิอากาศ	climate.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633

NO.	SERVER	URL	DIVISION	CONTACT	
35	ccexpert	ccexpert.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
36	การดำเนินงานลดก๊าซเรือนกระจกของประเทศ	mitigation.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
37	สำหรับดูสถานะของระบบที่ DCCE	ssmonitor2.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
38	สำหรับดูสถานะของระบบที่ GDCC	ssmonitor.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
39	โครงการแพลตฟอร์มกลางกรีนดิจิทัล Green Digital Platform พัฒนาในปี 2566	https://greenplatform.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
40	ระบบขออนุญาตจอดรถ	computer.dcce.go.th/car_cce	กลก.	ธไนศวรรย์ กุลบุตร	1632
41	เครื่องสำรองข้อมูล Green Platform	เครื่องสำรองข้อมูล Green Platform	กลก.	สุพรรณี สุวรรณชาติ	1620
42	NEW WEBSITE DCCE : เว็บไซต์กรมฯ พัฒนาปี 2567 (งบ 66 พลางก่อน)	dav.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
43	SCP	scpallgreen.dcce.go.th	กลก.	พิมพ์ใจ ธนะพิสิฐ	1620
44	ระบบบริหารจัดการองค์กร(Single Sign On)	sso.dcce.go.th	กลก.	ธไนศวรรย์ / โชคดี	1632
45	ระบบวิเคราะห์ข้อมูลสำหรับผู้บริหาร (BI)	bi.dcce.go.th	กลก.	โชคดี มั่นคง	1632
46	เอกสาร (Doc Office)	doc.dcce.go.th	กลก.	ธไนศวรรย์ กุลบุตร	1632
47	ระบบติดตามแผนงาน	eplan.dcce.go.th	กลก.	โชคดี มั่นคง	1632
48	SCP Data Center บริการข้อมูลและองค์ความรู้ที่เกี่ยวข้องกับการผลิต การบริการและการบริโภคที่เป็นมิตรกับสิ่งแวดล้อม	scpdatacenter.dcce.go.th	กลก.	พิมพ์ใจ ธนะพิสิฐ	1620
49	ระบบ enviportal	enviportal.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
50	ระบบ eservice2	eservice2.dcce.go.th	กลก.	จิรพรรณ เมืองปลื้ม	1620
51	ระบบรายงานการเพิ่มพื้นที่สีเขียวในเขตเมืองและชุมชน (ส่วนของระบบรายงาน)	e-report.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
52	เว็บไซต์ห้องสมุด	library.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
53	เว็บไซต์บริหารจัดการข้อมูลและสารสนเทศด้านขยะมูลฝอย (Infotrash)	infotrash.dcce.go.th	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
54	Thaigreenhotel	thaigreenhotel.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
55	webservice	webservice.dcce.go.th	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
56	แผนที่ข้อมูลเปิด (wms)	wms.dcce.go.th	กลก.	สุพรรณี สุวรรณชาติ	1620
57	ระบบจัดเก็บข้อมูลขยะของกรม	http://goffice.dcce.go.th/home/	กลก.	ไพลิน พันธุ์แน่น	1633
58	ระบบตรวจประเมินสำนักงานสีเขียว (สำหรับหน่วยงานและผู้ตรวจประเมิน)	greenoffice.dcce.go.th	กสร.	งามนิจ อนุศาสนี	1661
59	ระบบแผนที่ความรู้เครือข่าย ทสม.	tsmmap.dcce.go.th	กสร.	ฐิติยา คุณเดช	1846

NO.	SERVER	URL	DIVISION	CONTACT	
60	ระบบสารสนเทศเพื่อเฝ้าระวังและฟื้นฟูทรัพยากรธรรมชาติและสิ่งแวดล้อม - Web	http://nevt.dcce.go.th/	กสร.	ฐิติยา คุณเดช	1846
61	โครงการโรงแรมที่เป็นมิตรกับสิ่งแวดล้อม (Greenhotel)	https://greenhotel.dcce.go.th/	กสร.	ไพลิน พันธุ์แน่น	1633
62	ระบบสารสนเทศเพื่อเฝ้าระวังและฟื้นฟูทรัพยากรธรรมชาติและสิ่งแวดล้อม - Database	http://nevt.dcce.go.th/	กสร.	ไพลิน พันธุ์แน่น	1633
63	โครงการส่งเสริมการผลิตที่เป็นมิตรกับสิ่งแวดล้อม (Green Production)	greenproduction.dcce.go.th	กสร.	ธัญมน หมั่นกิจ	1661
64	ระบบฐานข้อมูลเครือข่ายเยาวชน	https://greenyouth.dcce.go.th/	กสร.	โศภิษฐ์ รัตนพันธุ์	1840
65	ระบบฐานข้อมูลลูกเสืออนุรักษ์ทรัพยากรธรรมชาติและสิ่งแวดล้อม	greenscout.dcce.go.th/	กสร.	โศภิษฐ์ รัตนพันธุ์	1840
66	ระบบการจัดการค่ายลูกเสือที่เป็นมิตรต่อสิ่งแวดล้อม	https://greenscout-interactive.dcce.go.th/	กสร.	ปนัดดา สมบูรณ์สวัสดี	1709
67	ระบบแผนที่ความรู้เครือข่าย ทสม.	nevtmap.dcce.go.th	กสร.	ฐิติยา คุณเดช	1846
68	ระบบการจัดการค่ายลูกเสือที่เป็นมิตรต่อสิ่งแวดล้อม	https://greenscout-interactive-admin.dcce.go.th/	กสร.	ปนัดดา สมบูรณ์สวัสดี	1709
69	ระบบร้านอาหารที่เป็นมิตรกับสิ่งแวดล้อม	greenrestaurant.dcce.go.th	กสร.	ศุภลักษณ์ ศรีลาวงษ์	1661
70	ฐานข้อมูลเอกสารในระบบคุณภาพ	qms.dcce.go.th	ศปส.	อัญชลี แท่นนิล	089-0145970
71	การเรียนรู้ผ่านสื่ออิเล็กทรอนิกส์	e-learning.dcce.go.th	ศปส.	อนงค์นาฏ อินสุธา	3620
72	ระบบเฝ้าระวังและเตือนภัยสภาพอากาศร้อนจัด	heatindex.dcce.go.th	ศปส.	วุฒิชัย แพงแก้ว	1124
73	ระบบการจัดการข้อมูลสำหรับห้องปฏิบัติการทางวิทยาศาสตร์	lims.dcce.go.th	ศปส.	อัญชลี แท่นนิล	089-0145970
74	ระบบเผยแพร่แลกเปลี่ยนแบ่งปันเพื่อการตั้งรับ ปรับตัว การเปลี่ยนแปลงสภาพภูมิอากาศ	http://thailandadaptationinfo.dcce.go.th	กปอ.	นางสาวมนพิสุทธิ์ แก้วศรี	1558
75	ระบบสารบรรณ 2566 (โครงสร้างใหม่)	https://office.dcce.go.th/saraban/	สลก.	อรุณ ทรัพย์ประเสริฐ	1646
76	ระบบสารสนเทศทรัพยากรบุคคล(Main)	dcce.dpis.go.th	สลก.	ไพลิน พันธุ์แน่น	1633
77	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก *** (ยังไม่ได้จด Domain)	GHGMicroservice c1	กลก.	อภิศักดิ์ วัฒนพงษ์	1991

NO.	SERVER	URL	DIVISION	CONTACT	
78	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGMicroservice c2	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
79	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก (DB)	GHGMSSQL	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
80	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGMicroservice c3	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
81	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGObj Storage	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
82	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGPostgres API	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
83	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGRabbitMQ	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
84	สร้างแพลตฟอร์มกลางการจัดเก็บฐานข้อมูลก๊าซเรือนกระจก	GHGRepository	กลก.	อภิศักดิ์ วัฒนพงษ์	1991
85	การลดก๊าซเลือนกระจกของประเทศไทย (รอจด Domin Name แทนตัวเก่า)	Mitigation_NEW_Uat	กลก.	ธนกฤต จันทร์ขำ	1603
86	การลดก๊าซเลือนกระจกของประเทศไทย	ev-gov.dcce.go.th	กลก.	ธนกฤต จันทร์ขำ	1603
87	การลดก๊าซเลือนกระจกของประเทศไทย DB	Mitigation_NEW_Db	กลก.	ธนกฤต จันทร์ขำ	1603
88	ระบบการบูรณาการข้อมูลสารสนเทศภูมิศาสตร์เพื่อใช้ร่วมกันในองค์กรระหว่างส่วนกลางและภูมิภาค	gis.dcce.go.th	กลก.	ไพลิน พันธุ์แน่น	1633
89	ระบบการจัดเก็บข้อมูล ISO/ICE	Pt.dcce.go.th	ศปส.	อัญชลี แท่นนิล	089-0145970

สถานภาพครุภัณฑ์คอมพิวเตอร์ กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ประจำปี พ.ศ. 2568

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งโปรแกรมพื้นฐานต่างๆ ที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ใช้ในการดำเนินงานปัจจุบันจะมีการสำรวจสภาพความพร้อมใช้และแผนในการจัดหา ทดแทนประจำทุกปี มีรายละเอียดดังตารางต่อไปนี้

ลำดับ	รายการครุภัณฑ์คอมพิวเตอร์	จำนวน	หมายเหตุ
1	เครื่องคอมพิวเตอร์แม่ข่าย (Server)	28	
2	เครื่องคอมพิวเตอร์ (PC)	658	
3	เครื่องคอมพิวเตอร์ (Notebook)	132	
4	เครื่องพิมพ์ชนิดเลเซอร์ (Laser Printer)	178	
5	เครื่องพิมพ์ชนิดฉีดหมึก (Inkjet Printer)	23	
6	เครื่องพิมพ์ชนิด Design jet	7	
7	เครื่องพิมพ์ชนิด Multifunction	34	
8	เครื่องสแกนเนอร์ (Scanner)สำหรับงานเก็บเอกสารทั่วไป	34	
9	เครื่องสำรองไฟฟ้า (UPS)	448	
10	Tablet	46	
11	โปรแกรมระบบปฏิบัติการ Windows	658	
12	โปรแกรม Microsoft Office	658	
13	SQL Server	1	
14	Windows Server	18	
15	V Sphere	2	
16	V Center	1	
17	Crystal Report	3	
18	โปรแกรมบริหารจัดการข้อมูลสารสนเทศภูมิศาสตร์บนโครงสร้างพื้นฐานภายในองค์กรระดับมาตรฐาน	1	
19	โปรแกรมบริหารจัดการข้อมูลสารสนเทศภูมิศาสตร์บนโครงสร้างพื้นฐานภายในองค์กรประเภทผู้ใช้งาน-ผู้เชี่ยวชาญสารสนเทศภูมิศาสตร์ระดับมาตรฐาน	2	

ตารางแสดงรายการเครื่องคอมพิวเตอร์และอุปกรณ์

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน สามารถแยกประเภทความเสี่ยงเป็น 5 ประเภท ดังนี้

1. ความเสี่ยงด้านเทคโนโลยีการเชื่อมต่อ หมายถึง ความเสี่ยงที่เกิดขึ้นจากการใช้งานเครือข่ายและระบบที่เชื่อมโยงกัน ไม่ว่าจะเป็นอินเทอร์เน็ต เครือข่ายภายในองค์กร หรืออุปกรณ์ IoT ซึ่งสามารถส่งผลกระทบต่อความปลอดภัย ข้อมูล หรือการดำเนินงานได้

2. ความเสี่ยงด้านช่องทางการให้บริการ หมายถึง หมายถึง ความเสี่ยงที่เกิดจากช่องทางต่าง ๆ ที่กรมใช้ในการให้บริการ เช่น เว็บไซต์, แอปพลิเคชัน, คอลเซ็นเตอร์, หรือโซเชียลมีเดีย ซึ่งอาจส่งผลต่อการใช้บริการ ความน่าเชื่อถือขององค์กร หรือการดำเนินงานโดยรวมได้

3. ความเสี่ยงด้านผลิตภัณฑ์และการให้บริการ หมายถึง ความเสี่ยงที่เกิดจากซอฟต์แวร์สำเร็จรูป หรือระบบซอฟต์แวร์ที่ใช้หรือมีในองค์กร เช่น ERP, CRM, HR, SCM, ระบบปฏิบัติการ, โปรแกรมประยุกต์, ฐานข้อมูล, และซอฟต์แวร์เฉพาะทางอื่นๆ เช่น ซอฟต์แวร์สำหรับการออกแบบ, ซอฟต์แวร์สำหรับการวิเคราะห์ข้อมูล

4. ความเสี่ยงด้านลักษณะเฉพาะขององค์กร หมายถึง ความเสี่ยงที่เกิดจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ เช่น ระบบหรือบริการด้านเทคโนโลยีสารสนเทศที่หน่วยงานใช้บริการจากผู้ให้บริการภายนอก Outsource/IT Outsource ที่มีสิทธิ์เข้าถึงระบบงานของหน่วยงาน ผู้ให้บริการ Web Hosting เป็นต้น

5. ความเสี่ยงจากการถูกคุกคามทางไซเบอร์ หมายถึง การกระทำโดยเจตนาของบุคคลหรือกลุ่มบุคคลที่พยายามเจาะระบบหรือทำลายความมั่นคงของระบบสารสนเทศ คอมพิวเตอร์ หรือเครือข่ายขององค์กรหรือบุคคล โดยมีวัตถุประสงค์หลายรูปแบบ เช่น ขโมยข้อมูล ล้วงความลับ ทำลายระบบ หรือเรียกค่าไถ่ เป็นต้น

ลักษณะรายละเอียดของความเสี่ยง (Description of risk)

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
1. ความเสี่ยงจากการเข้าถึงและใช้งานระบบเครือข่ายภายใน	ความเสี่ยงด้านเทคโนโลยีการเชื่อมต่อ	การเข้าถึงระบบเครือข่ายภายในหากไม่มีมาตรการควบคุมที่เหมาะสม อาจกลายเป็นช่องทางให้ผู้โจมตีเข้าถึงระบบเครือข่ายหลัก	- การเข้าถึงระบบภายใน โดยใช้งานอุปกรณ์ส่วนตัวที่ไม่มีการป้องกันที่เหมาะสม - การกำหนดค่า เช่น การเปิดพอร์ตที่ไม่จำเป็น หรือการตั้งค่าที่ไม่ได้เข้ารหัส - อุปกรณ์เครือข่ายที่ไม่ได้รับการบำรุงรักษา	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย/อุปกรณ์เครือข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
2. ความเสี่ยงในการให้บริการผ่าน **Website** หรือ **Web Application**	ความเสี่ยงด้านช่องทางการให้บริการ	**Website** หรือ **Web Application** ที่ให้บริการ อาจมีช่องโหว่และตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูล	- **Website** หรือ **Web Application** ที่จัดการข้อมูลผู้ใช้หรือข้อมูลสำคัญ มีช่องโหว่ - **Mobile Application** ที่มีการจัดการข้อมูลผู้ใช้ที่ไม่ปลอดภัย ขาดการเข้ารหัสข้อมูล หรือการเปิด **API** โดยไม่มีการควบคุม - บัญชี **Social Media** หรือ **Instant Messaging** ที่ใช้ขาดการตั้งรหัสผ่านที่มีความปลอดภัย	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย
3. ความเสี่ยงจากการใช้หรือมีผลิตภัณฑ์และระบบซอฟต์แวร์ในองค์กร	ความเสี่ยงด้านผลิตภัณฑ์และการให้บริการ	ผลิตภัณฑ์ที่จัดหา และระบบซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้หรือให้บริการในองค์กร อาจขาดการออกแบบด้านความปลอดภัยและทำให้อาจมีช่องโหว่และถูกโจมตี	- ซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้หรือให้บริการในองค์กรมีส่วนที่เขียนโค้ดผิดพลาด - การขาดการอัปเดตซอฟต์แวร์	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย
4. ความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้	ความเสี่ยงด้านลักษณะเฉพาะขององค์กร	ผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น เซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย อาจเป็นช่องทางที่ผู้โจมตีใช้เจาะระบบ	- ผู้ให้บริการ ที่มีสิทธิ์เข้าถึง เซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย ได้ไม่ได้รับอนุญาต - Outsource/IT Outsource ที่มีสิทธิ์เข้าถึงระบบงานโดยไม่ได้รับอนุญาต	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์ แม่ข่าย/อุปกรณ์ เครือข่าย

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง	ผู้ได้รับผลกระทบ
5. ความเสี่ยงจากการปฏิบัติงานภายใน และความน่าเชื่อถือขององค์กร	ความเสี่ยงจากการถูกคุกคามทางไซเบอร์	การถูกคุกคามทางไซเบอร์ส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่และความน่าเชื่อถือขององค์กร	- ระยะเวลาที่ระบบหยุดทำงานจากการถูกโจมตีทางไซเบอร์ - จำนวนและประเภทของช่องทางที่เคยถูกโจมตี	ผู้ใช้งาน ผู้ดูแลระบบ ผู้บริหารขององค์กร

การประมาณความเสี่ยง

โดยกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม กำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับความรุนแรง โอกาสที่จะเกิดความเสี่ยง ระดับความเสี่ยง ดังนี้

ระดับและโอกาสในการเกิดเหตุการณ์ต่าง ๆ			ระดับความรุนแรง (5 คะแนน)	
ระดับ	โอกาสที่จะเกิด	คำอธิบาย	ต่อระบบงาน	ต่อพันธกิจ
5	สูงมาก	5 ครั้ง/ปี	5	5
4	สูง	4 ครั้ง/ปี	4	4
3	ปานกลาง	3 ครั้ง/ปี	3	3
2	น้อย	2 ครั้ง/ปี	2	2
1	น้อยมาก	1 ครั้ง/ปี	1	1

ตารางแสดงการประมาณความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
1. ความเสี่ยงจากการเข้าถึงและใช้งานระบบเครือข่ายภายใน	ความเสี่ยงด้านเทคโนโลยีการเชื่อมต่อ	การเข้าถึงระบบเครือข่ายภายใน หากไม่มีมาตรการควบคุมที่เหมาะสม อาจกลายเป็นช่องทางให้ผู้โจมตีเข้าถึงระบบเครือข่ายหลัก	1	3
2. ความเสี่ยงในการให้บริการผ่าน Website หรือ Web Application	ความเสี่ยงด้านช่องทางการให้บริการ	Website หรือ Web Application ที่ให้บริการ อาจมีช่องโหว่และตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูล	5	3

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง
3. ความเสี่ยงจากการใช้หรือมีผลิตภัณฑ์และระบบซอฟต์แวร์ในองค์กร	ความเสี่ยงด้านผลิตภัณฑ์และการให้บริการ	ผลิตภัณฑ์ที่จัดหา และระบบซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้หรือให้บริการในองค์กรอาจขาดการออกแบบด้านความปลอดภัยและทำให้อาจมีช่องโหว่และถูกโจมตี	1	3
4. ความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้	ความเสี่ยงด้านลักษณะเฉพาะขององค์กร	- ผู้ให้บริการ ที่มีสิทธิ์เข้าถึง เซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย ได้ไม่ได้รับอนุญาต - Outsource/IT Outsource ที่มีสิทธิ์เข้าถึงระบบงาน โดยไม่ได้รับอนุญาต	5	5
5. ความเสี่ยงจากการปฏิบัติงานภายในและความน่าเชื่อถือขององค์กร	ความเสี่ยงจากการถูกคุกคามทางไซเบอร์	การถูกคุกคามทางไซเบอร์ส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่และความน่าเชื่อถือขององค์กร	2	3

การประเมินค่าความเสี่ยง

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยต่าง ๆ เช่น โอกาสที่จะเกิดภัยคุกคาม ระดับผลกระทบความรุนแรงที่มีต่อระบบ

ระดับความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง
1-5	ต่ำ	ยอมรับความเสี่ยง
6-10	ปานกลาง	ยอมรับความเสี่ยง
11-15	สูง	ควบคุมความเสี่ยง
16-20	สูงมาก	ควบคุมความเสี่ยง

ตารางแสดงการประเมินความเสี่ยง

ชื่อความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
1. ความเสี่ยงจาก การเข้าถึงและใช้งานระบบเครือข่ายภายใน	ความเสี่ยงด้านเทคโนโลยีการเชื่อมต่อ	การเข้าถึงระบบเครือข่ายภายใน หากไม่มีมาตรการควบคุมที่เหมาะสม อาจกลายเป็นช่องทางให้ผู้โจมตีเข้าถึงระบบเครือข่ายหลัก	1	3	4
2. ความเสี่ยงในการให้บริการผ่าน Website หรือ Web Application	ความเสี่ยงด้านช่องทางการให้บริการ	Website หรือ Web Application ที่ให้บริการ อาจมีช่องโหว่และตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูล	5	3	10
3. ความเสี่ยงจากการใช้หรือมีผลิตภัณฑ์และระบบซอฟต์แวร์ในองค์กร	ความเสี่ยงด้านผลิตภัณฑ์และการให้บริการ	ผลิตภัณฑ์ที่จัดหา และระบบซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้หรือให้บริการในองค์กร อาจขาดการออกแบบด้านความปลอดภัย และทำให้อาจมีช่องโหว่และถูกโจมตี	1	3	3
4. ความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้	ความเสี่ยงด้านลักษณะเฉพาะขององค์กร	- ผู้ให้บริการ ที่มีสิทธิ์เข้าถึง เซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย ได้ไม่ได้รับอนุญาต - Outsource/IT Outsource ที่มีสิทธิ์เข้าถึงระบบงาน โดยไม่ได้รับอนุญาต	5	5	15
5. ความเสี่ยงจากการปฏิบัติงานภายในและความน่าเชื่อถือขององค์กร	ความเสี่ยงจากการถูกคุกคามทางไซเบอร์	การถูกคุกคามทางไซเบอร์ส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่และความน่าเชื่อถือขององค์กร	2	3	6

การรายงานผลการวิเคราะห์ความเสี่ยง

จากผลการประเมินความเสี่ยง สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนี้

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
1	ความเสี่ยงจากการเข้าถึงและใช้งานระบบเครือข่ายภายใน	ความเสี่ยงด้านเทคโนโลยีการเชื่อมต่อ	การเข้าถึงระบบเครือข่ายภายใน หากไม่มีมาตรการควบคุมที่เหมาะสม อาจกลายเป็นช่องทางให้ผู้โจมตีเข้าถึงระบบเครือข่ายหลัก	4
2	ความเสี่ยงในการให้บริการผ่าน Website หรือ Web Application	ความเสี่ยงด้านช่องทางการให้บริการ	Website หรือ Web Application ที่ให้บริการ อาจมีช่องโหว่และตกเป็นเป้าหมายของการโจมตีเพื่อขโมยข้อมูล	10
3	ความเสี่ยงจากการใช้หรือมีผลิตภัณฑ์และระบบซอฟต์แวร์ในองค์กร	ความเสี่ยงด้านผลิตภัณฑ์และการให้บริการ	ผลิตภัณฑ์ที่จัดหา และระบบซอฟต์แวร์ที่พัฒนาขึ้นเพื่อใช้หรือให้บริการในองค์กร อาจขาดการออกแบบด้านความปลอดภัยและทำให้อาจมีช่องโหว่และถูกโจมตี	3
4	ความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้	ความเสี่ยงด้านลักษณะเฉพาะขององค์กร	- ผู้ให้บริการ ที่มีสิทธิ์เข้าถึง เซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย ได้ไม่ได้รับอนุญาต - Outsource/IT Outsource ที่มีสิทธิ์เข้าถึงระบบงานโดยไม่ได้รับอนุญาต	15
5	ความเสี่ยงจากการปฏิบัติงานภายใน และความน่าเชื่อถือขององค์กร	ความเสี่ยงจากการถูกคุกคามทางไซเบอร์	การถูกคุกคามทางไซเบอร์ส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่และความน่าเชื่อถือขององค์กร	6

การจัดการความเสี่ยง

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ 10 ขึ้นไป ส่วนความเสี่ยงที่มีระดับต่ำกว่า 10 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
1	ความเสี่ยงจากการเข้าถึงและใช้งานระบบเครือข่ายภายใน	4	ยอมรับความเสี่ยง	- กำหนดให้มีมาตรการควบคุมการใช้อุปกรณ์ส่วนตัวเชื่อมต่อระบบเครือข่ายภายใน - จำกัด **Remote Access** โดยใช้ **VPN** ที่เข้ารหัส และมีการยืนยันตัวตน และ - ปิดพอร์ตหรือบริการที่ไม่จำเป็นสำหรับการเข้าจากภายนอก - อัปเดตระบบปฏิบัติการ, ซอฟต์แวร์, และอุปกรณ์เครือข่ายให้เป็นเวอร์ชันล่าสุด	กลุ่มพัฒนาเทคโนโลยีดิจิทัล /กอง ขับเคลื่อนการลดก๊าซเรือกระจก	กย.69
2	ความเสี่ยงในการให้บริการผ่าน **Website** หรือ **Web Application**	10	ยอมรับความเสี่ยง	- ตรวจสอบและประเมินช่องโหว่ **Website** และ **Web Application** - กำหนดให้มีการเข้ารหัสข้อมูล หรือการควบคุมการเปิด **API** - ตั้งรหัสผ่านบัญชี **Social Media** หรือ **Instant Messaging** ที่มีความปลอดภัย และมีการเปลี่ยนรหัสผ่านเป็นระยะ เพื่อป้องกันการคาดเดารหัสผ่าน	กลุ่มพัฒนาเทคโนโลยีดิจิทัล /กอง ขับเคลื่อนการลดก๊าซเรือกระจก	กย.69
3	ความเสี่ยงจากการใช้หรือมีผลิตภัณฑ์และระบบซอฟต์แวร์ในองค์กร	3	ยอมรับความเสี่ยง	- กำหนดให้ผู้พัฒนาเขียนโค้ดโดยยึดหลักตามมาตรฐานที่ปลอดภัย - มีการทดสอบระบบ เช่น จำลองการโจมตีภายนอก - มีการตรวจสอบเวอร์ชันและช่องโหว่ของไลบรารีที่นำมาใช้	สำนัก/ศูนย์/กอง/ กลุ่มพัฒนาเทคโนโลยีดิจิทัล /กอง ขับเคลื่อน	กย.69

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาการปฏิบัติ
					การลดก๊าซเรือกระจก	
4	ความเสี่ยงจากผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้	15	ควบคุมความเสี่ยง	- ให้สิทธิ์การเข้าถึงเซิร์ฟเวอร์, ฐานข้อมูล หรือระบบเครือข่าย เฉพาะเท่าที่จำเป็น และปิดสิทธิ์ทันทีเมื่อเสร็จงาน - บังคับใช้ VPN และการยืนยันตัวตน 2 ชั้น (Multi-Factor Authentication)	กลุ่มพัฒนาเทคโนโลยีดิจิทัล /กอง ขับเคลื่อนการลดก๊าซเรือกระจก	กย.69
5	ความเสี่ยงจากการปฏิบัติงานภายในและความน่าเชื่อถือขององค์กร	6	ยอมรับความเสี่ยง	- ปฏิบัติขั้นตอนการรับมือหากเกิดเหตุการณ์ เช่น การแจ้งเตือน การกักกันระบบ การกู้คืน - ตรวจสอบ แก้ไข และป้องกันช่องโหว่ไม่ให้ถูกโจมตีซ้ำ - อบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์แก่เจ้าหน้าที่	สำนัก/ศูนย์/กอง/ กลุ่มพัฒนาเทคโนโลยีดิจิทัล /กอง ขับเคลื่อนการลดก๊าซเรือกระจก	กย.69

แผนบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้ผ่านการพิจารณาจากคณะทำงานบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม เพื่อให้เจ้าหน้าที่กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารต่อไป

(ลงชื่อ) .....

(นายปวิช เกศววงศ์)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)

กรมการเปลี่ยนแปลงสภาพภูมิอากาศและสิ่งแวดล้อม

๒๘ / พ.ค. / ๒๕๖๘