

เอกสารประกอบการตรวจเช็คห้องคอมพิวเตอร์เบื้องต้น



ใช่

- จัดหาพื้นที่ปลอดภัยเพื่อรองรับการย้ายอุปกรณ์ไอทีของท่านชั่วคราว เพื่อปรับปรุงห้องคอมพิวเตอร์ใหม่
- ในกรณีที่ต้องการปรับปรุงห้องคอมพิวเตอร์เดิม หรือสร้างห้องคอมพิวเตอร์ใหม่ ให้ติดต่อบริษัทผู้เชี่ยวชาญเป็นผู้ให้คำแนะนำทางเทคนิค
- พิจารณาการเช่าพื้นที่ห้องคอมพิวเตอร์ เพื่อดำเนินการปฏิบัติงานชั่วคราว

ไม่ใช่

ควรพิจารณาการตรวจเช็คห้องคอมพิวเตอร์ส่วนต่างๆ

3 ส่วน ดังนี้

1. สภาพแวดล้อมทั่วไปของห้องคอมพิวเตอร์
2. ระบบอุปกรณ์คอมพิวเตอร์
3. ระบบเครือข่ายเน็ตเวิร์ค

1. สภาพแวดล้อมทั่วไปของห้องคอมพิวเตอร์

รายการที่พิจารณา	ผลการตรวจสอบ		คำแนะนำเบื้องต้น
	ปกติ	มีข้อบกพร่อง	
1 สภาพแวดล้อมทางกายภาพทั้งภายใน และรอบห้องคอมพิวเตอร์ <ul style="list-style-type: none"> ตรวจสอบผลกระทบทางกายภาพที่มีต่อกำแพงหรือผนังโดยรอบห้องทั้งภายในและภายนอก ตรวจสอบประตูทางเข้าออกหลักสู่ห้องคอมพิวเตอร์สามารถใช้งานได้ตามปกติหรือไม่ ตรวจสอบและพิจารณาดมควันไฟพิษ มีร่องรอยของน้ำอยู่หรือไม่ และมีการหลุดร่อนของฉนวนจากพื้นหรือไม่ 			ทำความสะอาดห้องและกำแพงโดยรอบให้เรียบร้อย โดยให้มืออาชีพถ่ายเท
2 งานระบบไฟฟ้าพื้นฐานภายนอกห้องคอมพิวเตอร์ <ul style="list-style-type: none"> ตรวจสอบห้องเครื่องไฟฟ้าพื้นฐาน (หม้อแปลงไฟฟ้า, ตู้จ่ายไฟฟ้า) ของระบบห้องคอมพิวเตอร์ไดน้ำท่วมหรือไม่ ตรวจสอบเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉินไดน้ำท่วมหรือไม่ ตรวจสอบสายไฟหลักที่จ่ายให้แก่ห้องคอมพิวเตอร์ ได้รับผลกระทบจากน้ำท่วมหรือไม่ 			ถ้าระบบอุปกรณ์ไฟฟ้าหลักมีปัญหา ควรให้วิศวกรที่ชำนาญการเป็นผู้ตรวจสอบโดยละเอียด
3 งานระบบไฟฟ้าพื้นฐานภายในห้องคอมพิวเตอร์ <ul style="list-style-type: none"> ตรวจสอบสภาพทางกายภาพเบื้องต้นของอุปกรณ์หลักเช่น UPS, แบตเตอรี่ และตู้ไฟฟ้าย่อยในห้องอยู่ในสภาพปกติหรือไม่ ตรวจสอบสภาพทางกายภาพเบื้องต้นของตู้ระบบสายไฟฟ้าย่อยในห้องที่จ่ายให้แก่ตู้อุปกรณ์ไอทีต่างๆ รวมถึงเต้ารับไฟฟ้าพื้นฐาน รวมถึงสวิทช์เปิดปิดตามตำแหน่งต่างๆ ในพื้นที่ห้องคอมพิวเตอร์ รวมถึงสายป้อนไฟฟ้า อุปกรณ์อื่นๆ อาทิ เครื่องปรับอากาศ ระบบควบคุมสารดับเพลิง หรือระบบอื่นๆ อยู่ในสภาพปกติหรือไม่ ตรวจสอบระบบสายไฟฟ้าย่อยในห้องที่จ่ายให้แก่ตู้อุปกรณ์อื่นๆ อาทิ เครื่องปรับอากาศ ระบบควบคุมสารดับเพลิง หรือระบบอื่นๆ ไดน้ำท่วมหรือไม่ 			ถ้าระบบอุปกรณ์ UPS และแบตเตอรี่ มีปัญหาควรให้เจ้าของผลิตภัณฑ์เป็นผู้ตรวจสอบโดยละเอียด พร้อมทดสอบ Function การทำงานของอุปกรณ์
4 งานระบบปรับอากาศในห้องคอมพิวเตอร์ <ul style="list-style-type: none"> ตรวจสอบสภาพทางกายภาพของอุปกรณ์หลัก Condensing Unit ภายนอกอาคารอยู่ในสภาพปกติพร้อมใช้งานหรือไม่ ตรวจสอบสภาพทางกายภาพของอุปกรณ์เป่าลมเย็นของระบบปรับอากาศที่อยู่ในห้องคอมพิวเตอร์อยู่ในสภาพปกติพร้อมใช้งานหรือไม่ ในกรณีที่มิได้รับผลกระทบจากน้ำท่วม ให้ตรวจสอบความสามารถในการทำงานของอุปกรณ์ ในเรื่องการทำความเย็น และการควบคุมความชื้น จาก Record ของเครื่องปกติหรือไม่ 			ถ้าระบบอุปกรณ์ปรับอากาศ มีปัญหา ควรให้เจ้าของผลิตภัณฑ์เป็นผู้ตรวจสอบโดยละเอียด และให้ดูผลการดำเนินการทำความเย็น และการควบคุมความชื้น
5 งานระบบดับเพลิงในห้องคอมพิวเตอร์ <ul style="list-style-type: none"> หากห้องคอมพิวเตอร์มีการติดตั้งระบบสารดับเพลิงประเภท Gas หรือ Clean Agent แนะนำให้เรียกเจ้าของผลิตภัณฑ์เข้าทำการตรวจสอบโดยละเอียดก่อนเปิดใช้งานระบบว่าได้รับผลกระทบหรือไม่ 			

2. ระบบอุปกรณ์คอมพิวเตอร์

ในสภาวะหลังน้ำท่วม ถึงแม้ว่าอุปกรณ์คอมพิวเตอร์ของท่านอาจไม่ได้รับผลกระทบจากน้ำท่วมโดยตรง อย่างไรก็ตามอุปกรณ์คอมพิวเตอร์ซึ่งอยู่ในบริเวณน้ำท่วมเกินกว่า 48 ชั่วโมง จะมีความเสี่ยงที่เกิดจากความชื้นสูง ตลอดจนเชื้อราต่างๆ และสิ่งที่เราต้องคำนึงถึงคือน้ำที่มาจากน้ำท่วม ไม่ใช่ น้ำสะอาด สภาพความเป็นกรด-ด่าง อาทิ สารอินทรีย์ หรือสารเคมีต่างๆ สิ่งปนเปื้อน ที่มาจากน้ำเหล่านี้ เป็นสาเหตุที่ส่งผลกระทบต่ออุปกรณ์คอมพิวเตอร์ของเรา ซึ่งการตรวจสอบสภาพระบบอุปกรณ์คอมพิวเตอร์ ควรดำเนินการโดยผู้เชี่ยวชาญและมีความรู้เป็นอย่างดี

ไอบีเอ็ม ขอแนะนำเสนอการตรวจสอบระบบอุปกรณ์คอมพิวเตอร์เบื้องต้น ดังนี้

1. ทำการย้ายอุปกรณ์คอมพิวเตอร์ไปอยู่ในสภาพแวดล้อมที่เหมาะสม ควรมีความชื้นไม่เกิน 70 °F และความชื้นไม่เกิน 40% RH
2. ไม่ทำการเปิดอุปกรณ์คอมพิวเตอร์ที่โดนน้ำท่วมโดยตรง หรือไม่แน่ใจว่าถูกน้ำท่วม ให้ทำการถอดปลั๊กไฟฟ้า และติดต่อบริษัทผู้ดูแลอุปกรณ์คอมพิวเตอร์เหล่านั้นให้ดำเนินการตรวจสอบและแก้ไขต่อไป
3. สำหรับอุปกรณ์คอมพิวเตอร์ที่ไม่ได้ถูกน้ำท่วม ควรทำการตรวจสอบสภาพภายนอก และตรวจสอบสภาพร่องรอยความเสียหายทางกายภาพ โดยแนวทางการตรวจสอบเบื้องต้นได้แก่
 - ไม่มีคราบเกลือหรือออกไซด์ในบริเวณที่เป็นโลหะโดยเฉพาะในช่วงรอยต่อ
 - ไม่มีคราบน้ำหรือสนิมที่แผงวงจรต่างๆ ทั้งภายในและภายนอก
 - ไม่มีร่องรอยแตกหักเสียหาย ตลอดจนไม่มีไอน้ำในบริเวณหน้าปิดแสดงผลต่างๆ
 - สติกเกอร์หรือฉลากต่างๆ บนอุปกรณ์ไม่หลุดลอกหรือลบเลือน
 - ปุ่มกดหรือสวิทช์วงจรต่างๆ สามารถทำงานได้ตามปกติ
4. สำหรับเทปข้อมูล ฮาร์ดดิสก์ที่เก็บข้อมูล รวมถึงดิสก์ที่อยู่ในอุปกรณ์คอมพิวเตอร์ หากโดนน้ำไม่ควรทำการเช็ด เป่าแห้ง หรือนำออกด้วยตัวเอง ควรเก็บอุปกรณ์คอมพิวเตอร์เหล่านี้ไว้ในที่ปลอดภัย และติดต่อผู้เชี่ยวชาญเพื่อดำเนินการแก้ไขต่อไป
5. ควรรวบรวมและเตรียมข้อมูล backup ให้พร้อมสำหรับการฟื้นฟู ไม่ควรนำดิสก์ที่เปียกน้ำหรือมีความชื้นมาใช้งาน เพราะอาจทำให้ข้อมูลเสียหายจนไม่สามารถกู้คืนระบบมาได้
6. เมื่อทำการตรวจสอบสภาพภายนอกจนมั่นใจแล้ว ให้ทำการเปิดเครื่อง ตรวจสอบไฟแสดงผล เสียงเตือน การหมุนของหัวอ่านข้อมูล ตลอดจน error messages ต่างๆ บนอุปกรณ์คอมพิวเตอร์ว่ามีอะไรผิดปกติ
7. เนื่องจากความเสียหายบางกรณีไม่สามารถมองเห็นได้จากภายนอก และการตรวจสอบในแต่ละครั้งอาจต้องทำถึงระดับ Operating System เพื่อให้ข้อมูลเกิดความเสียหาย ถ้าท่านไม่มั่นใจในการทำงานของระบบอุปกรณ์คอมพิวเตอร์ ควรติดต่อผู้เชี่ยวชาญให้ทำการตรวจสอบโดยละเอียด

3. ระบบเครือข่ายเน็ตเวิร์ค

ในสภาวะหลังน้ำท่วม ควรทำการตรวจสอบระบบเครือข่ายให้สามารถทำงานได้ตามปกติ สำหรับอุปกรณ์ระบบเครือข่ายที่มีความเสี่ยง จำเป็นต้องทำการย้ายอุปกรณ์ระบบเครือข่ายไปยังสถานที่ที่เหมาะสม เพื่อทำการตรวจสอบร่องรอยความเสียหายทางกายภาพ และ error messages และไม่ควรรื้ออุปกรณ์ระบบเครือข่ายที่ถูกน้ำท่วมโดยตรง

ไอบีเอ็ม ขอแนะนำเสนอการตรวจสอบระบบเครือข่ายเน็ตเวิร์คเบื้องต้น ดังนี้

1. เตรียมอุปกรณ์ power supply เพื่อสำรองไว้ใช้งาน ในกรณีที่อุปกรณ์ power supply ของระบบเครือข่ายได้รับความเสียหายจากน้ำท่วมหรือความชื้น
2. ทดสอบการเชื่อมต่อโดยการ Ping จากระบบเซิร์ฟเวอร์ไปยัง Gateway วิธีการนี้เป็นการตรวจสอบเบื้องต้นว่าระบบเครือข่ายยังสามารถทำงานได้
3. สำหรับระบบเครือข่ายขนาดใหญ่ จำเป็นต้องทำการตรวจสอบว่ามีปัญหา blackholes หรือ sub-optimal routing ที่เกิดจากอุปกรณ์เครือข่ายบางตัวเสียหาย ซึ่งวิธีการทดสอบทำได้โดยการตรวจสอบเช็คตารางเส้นทาง (routing table) ว่าถูกต้องครบถ้วนหรือไม่
4. เนื่องจากน้ำท่วมอาจทำความเสียหายแก่สายเคเบิลภายในอาคารหรือภายในสำนักงาน ซึ่งทำให้ยากต่อการตรวจสอบ อาจต้องพิจารณาทางเลือกชั่วคราว เช่น การใช้ระบบ Wireless หรือ การทำงานระยะไกล โดยใช้ระบบ Virtual Private Network (VPN)
5. ระบบเครือข่ายเป็นการเชื่อมโยงของอุปกรณ์คอมพิวเตอร์จำนวนมาก อาจมีผลกระทบบางประการที่ไม่สามารถตรวจสอบได้ในเบื้องต้น จำเป็นต้องมีการติดต่อผู้เชี่ยวชาญ เพื่อทำการตรวจสอบการทำงานของระบบเครือข่ายทั้งหมดโดยละเอียด

นอกจากนี้ ไอบีเอ็ม มีทีมบริการผู้เชี่ยวชาญด้านการดูแลความต่อเนื่องของระบบธุรกิจและการกู้คืนระบบไอที (Business Resiliency and Disaster Recovery) ที่จะช่วยตรวจสอบว่าธุรกิจของท่านมีความเตรียมพร้อมในการรับมือกับความเสียหายมากเพียงใด รวมถึงช่วยประเมินวิเคราะห์ และวางแผน จัดการความเสี่ยงของระบบไอที

ขอบเขตการประเมินระบบเบื้องต้นประกอบด้วย

- การตรวจวิเคราะห์ผลกระทบทางธุรกิจของท่าน ในกรณีที่เหตุการณ์ไม่คาดคิด
- การประเมินศักยภาพในการกู้คืนระบบขององค์กร (Disaster Recovery Capability)
- การประเมินความพร้อมในการวางแผนสร้างความต่อเนื่องของธุรกิจ (Business Continuity Plan – BCP) และการวางแผนการกู้คืนระบบ (Disaster Recovery Plan – DRP) ทั้งกระบวนการและการปฏิบัติจริง
- การให้คำปรึกษาเพื่อช่วยให้ธุรกิจของท่านมีความพร้อม ในการรับมือกับสถานการณ์ที่ไม่คาดคิด