Work From Home
ให้ปลอดภัย รอดพ้นจากภัยไซเบอร์ (ตอนที่ 2)

6. การสำรองข้อมูลและการกู้คืนจากภัยพิบัติ

กำหนดวิธีปฏิบัติและฝึกอบรมให้บุคลากรเข้าใจและตระหนักถึงการปฏิบัติตามนโยบายการสำรองข้อมูลและการกู้คืนข้อมูลในกรณีทำงานที่บ้าน รวมทั้งการสำรองข้อมูลสำคัญในช่องทางส่วนกลางขององค์กรเพื่อให้สามารถกู้คืนได้

7. ความเสี่ยงจากการประชุมออนไลน์

การประชุมออนไลน์มีความเสี่ยงในการเข้าถึงข้อมูลและไฟล์ที่เป็นความลับโดยไม่ได้รับอนุญาต ควรมีการระมัดระวังการเผยแพร่รหัสผ่านของการประชุมออนไลน์ การเข้าถึงเครือข่าย WiFi การแชร์ไฟล์ที่เป็นอันตราย (Malicious) การเข้าถึงข้อมูลธุรกิจที่ละเอียดอ่อน และการมีผู้บุกรุกเข้ามาในการประชุม

8. ความเสี่ยงออนไลน์อื่น ๆ

ควรกำหนดนโยบายความปลอดภัยการทำงานที่บ้านและวิธีปฏิบัติ ให้ครอบคลุมความเสี่ยงข้างต้น และฝึกอบรมบุคลากรให้รู้เข้าใจปฏิบัติตามได้ถูกต้อง

9. การแชร์ไฟล์และการส่งข้อความ

- E-mail ธุรกิจไม่ควรใช้ในเครื่องคอมพิวเตอร์ส่วนตัว
- File Transfer Protocol ที่ปลอดภัย
- การใช้บริการคลาวด์ที่ปลอดภัย
- ไม่แชร์ข้อมูลธุรกิจผ่าน text massage หรือ แชท
- ฝึกอบรมบุคลากรให้เข้าใจในการแชร์ข้อมูล/ไฟล์ที่เหมาะสม

10. ความปลอดภัยของสภาพแวดล้อมในพื้นที่ทำงานที่บ้าน

กำหนดนโยบายความปลอดภัยการทำงานที่บ้าน โดยคำนึงถึงความปลอดภัยทางกายภาพ, การสอดแนมทางดิจิทัล, ความเป็นส่วนตัว, Social engineering, การลักลอบใช้บัญชี รวมทั้งขั้นตอนการเริ่มทำงานและออกจากงานในกรณีทำงานที่บ้าน

11. การลบทำลายอย่างปลอดภัย

กำหนดนโยบายการทำงานที่บ้านเกี่ยวกับการลบทำลายข้อมูลอย่างปลอดภัย ไม่ว่าจะเป็นข้อมูลในอุปกรณ์จัดเก็บข้อมูลคอมพิวเตอร์ อุปกรณ์ IoT สำเนาเอกสาร ซึ่งรวมถึงการกำกับดูแลการลบทำลาย

12. การบริหารความเสี่ยงการทำงานนอกสำนักงานและที่บ้าน

1. กำหนดความเสี่ยงเป็นระดับสูง
2. กำหนดนโยบายและขั้นตอนการปฏิบัติ
3. ต้องฝึกอบรมเป็นประจำ
4. มีการแจ้งเตือนเพื่อสร้างความรู้ความเข้าใจต่อเนื่อง
5. ประเมินความเสี่ยงและทบทวนสม่ำเสมอ
6. การกำกับดูแลผู้รับบริการ ซึ่งมีความเสี่ยงจากการทำงานที่บ้านเช่นกัน
7. มีการตรวจสอบโดยฝ่ายตรวจสอบภายใน
8. พิจารณาซื้อประกัน Cyber Liability Insurance

Scan QR Code
บทความฉบับเต็ม

ที่มา : ตลาดหลักทรัพย์แห่งประเทศไทย
(https://www.set.or.th/set/enterprise/article/detail.do?contentId=7694)