แนวปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของสำนักงานพัฒนาฝีมือแรงงานเลย

ลำดับ	ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๑	RIT๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	- สร้างความตระหนักในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ในส่วนของข้อมูลส่วนบุคคล - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย												
๒	RIT๐๓ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- ปรับปรุงแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)												
๓	RIT๐๔ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	- ตรวจสอบการตั้งค่าของ firewall อย่างสม่ำเสมอ - ตรวจสอบระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้ง อัพเดท patchโปรแกรมป้องกันไวรัส และ ระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ												
๔	RIT๐๕ ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	- ปรับปรุงโครงสร้างศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม												

แนวปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของสำนักงานพัฒนาฝีมือแรงงานเลย

ลำดับ	ความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
๕	RIT๐๗ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	- ปรับปรุงแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการ ขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ												
๖	RIT๑๐ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	- หาวิธีการป้องกันสัตว์ฟันแทะอุปกรณ์และตรวจเช็คเครื่องมือ และอุปกรณ์ทางกายภาพ อย่างสม่ำเสมอ - จัดทำแผนการตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์อย่างสม่ำเสมอ												
๗	RIT๑๑ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	- ตรวจสอบการเข้าออกของบุคคลภายนอก - ตรวจเช็ค การเปิด-ปิด การใช้อาคารทุกครั้ง												