เอกสารผลงาน

การบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย
สำนักงานปลัดกระทรวงแรงงาน

โดย

นางสาวจุฑารัตน์ สบู่ม่วง
ตำแหน่ง นักวิชาการคอมพิวเตอร์ 6ว

ผู้ขอรับการประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่ง นักวิชาการคอมพิวเตอร์ 7วช
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงแรงงาน

บทคัดย่อ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงแรงงาน เป็นหน่วยงานที่ดูแล กำกับการใช้งานทางด้านเทคโนโลยีสารสนเทศและการสื่อสารในภาพรวมของกระทรวงแรงงาน โดยปฏิบัติงานตามแผนแม่บทด้านแรงงาน (พ.ศ. 2550-2554) ที่เกี่ยวข้องในยุทธศาสตร์ที่ 5 การพัฒนาระบบฐานข้อมูลสารสนเทศด้านแรงงาน และยุทธศาสตร์ที่ 6 การพัฒนาการบริหารจัดการของกระทรวงแรงงานให้มีความเป็นเลิศ เพื่อให้การดูแล ควบคุมการปฏิบัติงานด้านการรักษาความปลอดภัยข้อมูล ระบบฐานข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่ายของกระทรวงแรงงาน สำหรับวัตถุประสงค์การจัดทำผลงานฉบับนี้ เพื่ออธิบายเกี่ยวกับคุณสมบัติและการทำงานของระบบงานหรืออุปกรณ์ต่าง ๆ ในภาพรวม ที่ติดตั้งใช้งานในห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย เพื่อรองรับภารกิจและการพัฒนางานทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามโครงการจัดทำห้องศูนย์ปฏิบัติการข้อมูลข่าวสารกลางของสำนักงานปลัดกระทรวงแรงงาน (Server Room) ปีงบประมาณ 2550 โดยมีการดำเนินงานจัดทำห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ครอบคลุมงาน ดังต่อไปนี้

1) ระบบสำรองไฟฟ้าอย่างต่อเนื่อง (UPS)
2) เครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน (Generator)
3) เครื่องปรับอากาศแบบควบคุมความชื้น (Precision Air)
4) ระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector)
5) ระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System)
6) ระบบดับเพลิงอัตโนมัติพร้อมระบบตรวจจับควันไฟความไวสูง
7) ระบบรักษาความปลอดภัยประตูทางเข้า-ทางออก (Access Control)
8) ระบบกล้องวงจรปิด
9) ระบบสายสัญญาณ (Cabling System)
10) การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย
11) การกำหนดสิทธิในการเข้าถึงข้อมูลในระบบสารสนเทศ
12) กระบวนการสำรองและกู้คืนข้อมูลสารสนเทศ สำนักงานปลัดกระทรวงแรงงาน

ผลของการดำเนินงานโครงการ ทำให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ที่มีความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมอยู่ในระดับมาตรฐานสากล พร้อมมีข้อเสนอแนะสำหรับบริหารจัดการด้านความมั่นคงปลอดภัยของข้อมูลอย่างต่อเนื่อง เห็นควรจัดหาบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านของการรักษาความมั่นคงปลอดภัยมาปฏิบัติหน้าที่เฝ้าระวังด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายภายในสำนักงานปลัดกระทรวงแรงงานประจำที่ (Monitoring) จะทำให้หน่วยงานมีระบบคอมพิวเตอร์และเครือข่ายที่มีความเสถียรภาพและประสิทธิภาพสามารถรองรับภารกิจของหน่วยงานได้อย่างดี

คำนำ

เอกสารการบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย สำนักงานปลัดกระทรวงแรงงาน ฉบับนี้จัดทำขึ้น เพื่อเป็นคู่มือการใช้งานอุปกรณ์หรือระบบงานทุกระบบในภาพรวม โดยเอกสารฉบับนี้แบ่งเป็น 2 ส่วน คือ ส่วนที่ 1 ผลงานที่เป็นผลการดำเนินงานที่ผ่านมาได้ให้ชื่อหัวข้อว่า "การบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย สำนักงานปลัดกระทรวงแรงงาน" และส่วนที่ 2 ข้อเสนอแนวความคิด/วิธีการ เพื่อพัฒนางานหรือปรับปรุงงานของหน่วยงานที่จะประเมินเพื่อแต่งตั้งให้มีประสิทธิภาพมากขึ้น โดยใช้หัวข้อว่า "ระบบป้องกันภัยคุกคามเครื่องคอมพิวเตอร์และระบบเครือข่าย"

ผู้จัดทำเอกสารฉบับนี้ ขอขอบพระคุณผู้บริหารทุกระดับ พี่ๆ เพื่อนและน้องทุกคนและหน่วยงานมา ณ โอกาสนี้ ที่ได้สนับสนุนส่งเสริมทำให้การดำเนินงานสำเร็จลุล่วง และหวังเป็นอย่างยิ่งว่าคู่มือการใช้อุปกรณ์หรือระบบงานในภาพรวมนี้จะมีประโยชน์ต่อหน่วยงานในการพัฒนาปรับปรุงงานให้มีประสิทธิภาพและประสิทธิผลยิ่งขึ้นต่อไป

นางสาวจุฑารัตน์ สบู่ม่วง
นักวิชาการคอมพิวเตอร์ 6ว
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

ส่วนที่ 1

ผลงานที่เป็นผลการดำเนินงานที่ผ่านมา

เรื่อง การบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

สำนักงานปลัดกระทรวงแรงงาน

ผลงานที่เป็นผลการดำเนินงานที่ผ่านมา

1. **ชื่อผลงาน** การบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย สำนักงานปลัดกระทรวงแรงงาน
2. **ระยะเวลาที่ดำเนินการ** ปีงบประมาณ 2550
3. **ความรู้ทางวิชาการหรือแนวความคิดที่ใช้ในการดำเนินการ**

การบริหารจัดการห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย สำนักงานปลัดกระทรวงแรงงาน นำกรอบความรู้ทางวิชาการหรือแนวความคิดมาประยุกต์ใช้ในการดำเนินงาน ประกอบด้วย

3.1 การควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและระบบป้องกันความเสียหายต่าง ๆ

แนวทางปฏิบัติ

1. **การควบคุมห้องคอมพิวเตอร์แม่ข่าย**
   - ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในห้องคอมพิวเตอร์แม่ข่ายหรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (computer operator) เจ้าหน้าที่ดูแลระบบ (system administrator) เป็นต้น
   - ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ห้องคอมพิวเตอร์แม่ข่ายควบคุมดูแลการทำงานตลอดเวลา เป็นต้น
   - ต้องมีระบบเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่าย โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
   - ควรจัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (network zone) ส่วนเครื่องแม่ข่าย (server zone) ส่วนเครื่องพิมพ์ (printer zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น นอกจากนี้ ควรแยกส่วนที่ต้องมีการเข้าถึงโดยเจ้าหน้าที่หลายฝ่ายออกจากห้องคอมพิวเตอร์แม่ข่าย เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่างๆ เป็นต้น

2. การป้องกันความเสียหาย

2.1 ระบบป้องกันไฟไหม้

- ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
- ห้องคอมพิวเตอร์แม่ข่ายหลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับห้องคอมพิวเตอร์แม่ข่ายสำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

2.2 ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟ
- ต้องมีระบบไฟฟ้าสำรองสำหรับระบบคอมพิวเตอร์สำคัญ เพื่อให้การดำเนินงานมีความต่อเนื่อง

2.3 ระบบควบคุมอุณหภูมิและความชื้น

- ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

2.4 ระบบเตือนภัยน้ำรั่ว

- ในกรณีที่มีการยกระดับพื้นของห้องคอมพิวเตอร์แม่ข่าย เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ก็ควรติดตั้งระบบเตือนภัยน้ำรั่ว บริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา นอกจากนี้ หากห้องคอมพิวเตอร์แม่ข่ายตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ก็ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่อย่างสม่ำเสมอ

3.2 การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)

วัตถุประสงค์

การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (access risk) หรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

แนวทางปฏิบัติ

1. <u>การบริหารจัดการข้อมูล</u>

- ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น
- ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (storage) นำเข้า (input) ประมวลผล (operate) และแสดงผล (output) นอกจากนี้ ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (distributed database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
- ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2. <u>การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน[1] (user privilege)</u>

- ต้องกำหนดสิทธิการใช้ข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (application system) สิทธิการใช้งานอินเตอร์เนต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิเฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ในกรณีมีความจำเป็นต้องใช้ user ที่มีสิทธิพิเศษ[2] ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม user ที่มีสิทธิพิเศษมีความรัดกุมเพียงพอหรือไม่นั้น หน่วยงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
  - ควรควบคุมการใช้งาน user ที่มีสิทธิพิเศษอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งาน user ดังกล่าวในลักษณะ dual control โดยให้เจ้าหน้าที่ 2 ราย ถือรหัสผ่านคนละครึ่ง หรือเก็บซอง password ไว้ในตู้เซฟ เป็นต้น และจำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
  - ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

---

[1] ผู้ใช้งาน หมายถึง เจ้าของข้อมูล ผู้บริหารระบบ (system administrator) เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (computer operator) เจ้าหน้าที่พัฒนาระบบ (system developer) และเจ้าหน้าที่อื่นที่ใช้งานระบบคอมพิวเตอร์

[2] User ที่มีสิทธิพิเศษ หมายถึง Root หรือ User อื่นที่มีสิทธิสูงสุด

- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิและหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (log out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น
- ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ share files เป็นต้น จะต้องเป็นการให้สิทธิเฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น ให้มีสิทธิใช้งานระบบคอมพิวเตอร์ในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3. <u>การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)</u>

- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิการเข้าใช้งานของผู้ใช้งาน (identification and authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี user account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น สำนักงานจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
  - ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 6 ตัวอักษร
  - ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น
  - สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน
    ส่วนผู้ใช้งานที่มีสิทธิพิเศษ เช่น ผู้บริหารระบบ (system administrator) และผู้ใช้งานที่ติดมากับระบบ (default user) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน
  - ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย
  - ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456” เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
  - ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 5 ครั้ง
- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

○ ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีต้องมีระบบการเข้ารหัส (encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

○ ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญ[3] อย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิใช้งานระบบแล้ว เช่น บัญชีรายชื่อของเจ้าหน้าที่หรือพนักงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (default user) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น disable ลบออกจากระบบ หรือ เปลี่ยน password เป็นต้น

4. <u>การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)</u>

○ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

○ ต้องเปิดใช้บริการ (service) [4] เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติม

○ ต้องดำเนินการติดตั้ง patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (system software) เช่น ระบบปฏิบัติการ DBMS และ web server เป็นต้น อย่างสม่ำเสมอ

○ ควรทดสอบ system software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

○ ควรมีแนวทางปฏิบัติในการใช้งาน software utility เช่น personal firewall password cracker เป็นต้น และตรวจสอบการใช้งาน software utility อย่างสม่ำเสมอ

○ ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

---

[3] ระบบงานสำคัญ หมายถึง ระบบงานต่าง ๆ ที่ให้บริการประชาชน เช่น ระบบเว็บไซต์กระทรวงแรงงาน และระบบงานภายในเครือข่าย เช่น ระบบสารบรรณ เป็นต้น

[4] บริการ (service) หมายถึง บริการต่าง ๆ ของเครื่องแม่ข่าย เช่น telnet, ftp, ping เป็นต้น

5. <u>การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)</u>

- ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายใน ส่วนเครือข่ายภายนอก ส่วน DMZ เป็นต้น
- ต้องมีระบบป้องกันการบุกรุก เช่น firewall เป็นต้น ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก
- ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยอย่างน้อยต้องมีการตรวจสอบในเรื่องดังต่อไปนี้อย่างสม่ำเสมอ
  - ความพยายามในการบุกรุกผ่านระบบเครือข่าย
  - การใช้งานในลักษณะที่ผิดปกติ
  - การใช้งาน และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- ต้องจัดทำแผนผังระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า parameter ต่างๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (physical disconnect) และจุดเชื่อมต่อ (disable port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง
- ในกรณีที่มีการเข้าถึงระบบเครือข่ายในลักษณะ remote access หรือการเชื่อมต่อเครือข่ายภายนอกโดยใช้ modem (dial out) ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และมีการควบคุมอย่างเข้มงวด เช่น การใช้ระบบ call back การควบคุม การเปิดปิด modem การตรวจสอบตัวตนจริงและสิทธิของผู้ใช้งาน การบันทึกรายละเอียดการใช้งาน และในกรณี dial out ก็ควรตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อออกจากระบบเครือข่ายภายใน เป็นต้น รวมทั้งต้องตัดการเชื่อมต่อการเข้าถึงดังกล่าวเมื่อไม่ใช้งานแล้ว
- ควรกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ก็ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- การใช้เครื่องมือต่างๆ (tools) เพื่อตรวจเช็คระบบเครือข่าย ควรได้รับการอนุมัติจากผู้มีอำนาจหน้าที่ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. การป้องกันไวรัส และ malicious code

- ต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้เป็นปัจจุบันอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น
- ฝ่ายคอมพิวเตอร์ควรจัดทำคู่มือในการป้องกันไวรัสให้แก่ผู้ใช้งานเพื่อใช้เป็นแนวทางปฏิบัติ รวมทั้งแจ้งและให้ความรู้แก่ผู้ใช้งานเกี่ยวกับไวรัสชนิดใหม่ๆ อย่างสม่ำเสมอ
- ควรควบคุมมิให้ผู้ใช้งานระงับการใช้งาน (disable) ระบบป้องกันไวรัสที่ได้ติดตั้งไว้ และควรแจ้งบุคคลที่เกี่ยวข้องทันทีในกรณีที่พบว่ามีไวรัส

7. บันทึกเพื่อการตรวจสอบ (audit logs)

- ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (login-logout logs) บันทึกการพยายามเข้าสู่ระบบ (login attempts) บันทึกการใช้ command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน
- ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

3.3 การสำรองข้อมูลระบบคอมพิวเตอร์ (Backup Plan)

วัตถุประสงค์

การสำรองข้อมูลระบบคอมพิวเตอร์ มีวัตถุประสงค์เพื่อให้มีข้อมูลระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา

แนวทางปฏิบัติ

การสำรองข้อมูลระบบคอมพิวเตอร์

1. การสำรอง
    - ต้องสำรองข้อมูลสำคัญ รวมถึงโปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง
    - ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยอย่างน้อยควรมีรายละเอียด ดังนี้

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อบันทึก (media)
- จำนวนที่ต้องสำรอง (copy)
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึก

○ ควรมีการบันทึกการปฏิบัติงาน (log book) เกี่ยวกับการสำรองข้อมูลของเจ้าหน้าที่ เพื่อตรวจสอบความถูกต้องครบถ้วน และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

2. การทดสอบ

○ ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

○ ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

3. การเก็บรักษา

○ ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในข้อ Physical Security ด้วย

○ ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ก็ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

○ ควรติดฉลากที่มีรายละเอียดชัดเจนไว้บนสื่อบันทึกข้อมูลสำรอง เพื่อให้สามารถค้นหาได้โดยเร็ว และเพื่อป้องกันการใช้งานสื่อบันทึกผิดพลาด

○ การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้มีอำนาจหน้าที่ และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยควรมีรายละเอียดเกี่ยวกับผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลา

○ ควรมีขั้นตอนการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้ว ซึ่งรวมถึงข้อมูลสำคัญต่างๆ ในฮาร์ดดิสก์ที่ยังค้างอยู่ใน recycle bin

3.4 การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นอาจก่อให้เกิดความเสี่ยงต่อหน่วยงานในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติของหน่วยงานเอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้หน่วยงานใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

แนวทางปฏิบัติ

1. <u>การคัดเลือกผู้ให้บริการ</u>

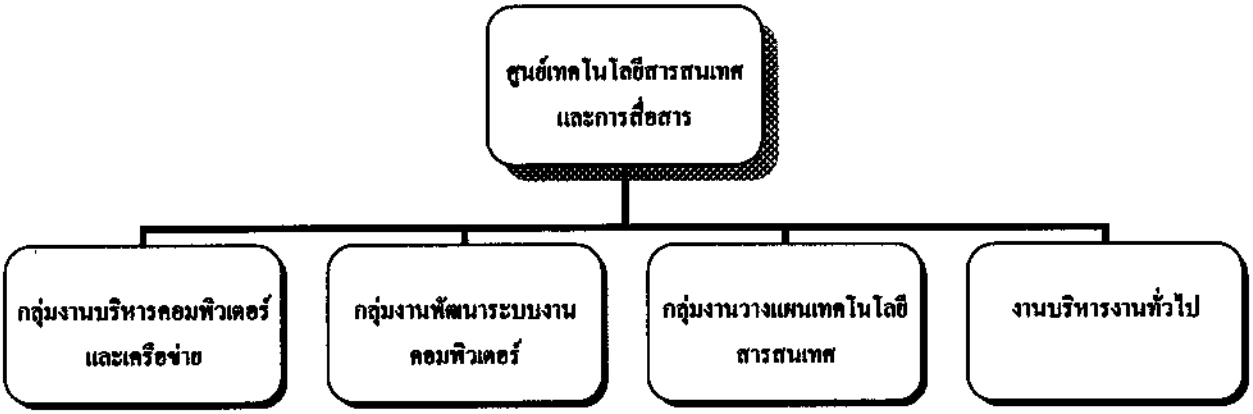
- ควรมีการกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ
- ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

2. <u>การควบคุมผู้ให้บริการ</u>

- ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้เจ้าหน้าที่บริษัทควบคุมดูแลการทำงานของผู้ให้บริการอย่างใกล้ชิดในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่หน่วยงาน (onsite service) และให้เจ้าหน้าที่หน่วยงานตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียดในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิด modem ทันทีที่การให้บริการเสร็จสิ้น เป็นต้น
- ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ
- ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่างๆ และแนวทางแก้ไข
- ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ

4. <u>สรุปสาระและขั้นตอนการดำเนินการ</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานในสังกัดสำนักงานปลัดกระทรวงแรงงาน ที่ตั้งขึ้นเพื่อรองรับและสนับสนุนภารกิจของหน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีอำนาจหน้าที่ ครอบคลุม ภารกิจในการจัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงให้สอดคล้องกับมาตรฐานกลางและนโยบายเทคโนโลยีสารสนเทศและการสื่อสารระดับประเทศ พัฒนาระบบงานคอมพิวเตอร์และเครือข่าย รวมทั้งให้คำปรึกษา แนะนำหรือฝึกอบรมการใช้คอมพิวเตอร์และการใช้งานโปรแกรม ดำเนินการเกี่ยวกับบริหารจัดการข้อมูลข่าวสาร เทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานในสังกัด และดูแลรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของกระทรวงแรงงาน มีโครงสร้างการบริหารงาน ประกอบด้วย งานบริหารทั่วไป กลุ่มงานบริหารคอมพิวเตอร์และเครือข่าย กลุ่มงานพัฒนาระบบงานคอมพิวเตอร์ และกลุ่มงานวางแผนเทคโนโลยีสารสนเทศ



<u>วิสัยทัศน์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร</u> : เป็นองค์กรกลางในการบริหารจัดการระบบสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายของกระทรวงแรงงานที่มีประสิทธิภาพ

สถานที่ดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเดิม ตั้งอยู่ ณ อาคารกระทรวงแรงงาน ชั้น 15 มีพื้นที่ประมาณ 582 ตารางเมตร โดยพื้นที่หนึ่งในสาม เป็นพื้นที่ห้องสมุดสำนักงานปลัดกระทรวงแรงงาน ส่วนที่เหลือประกอบด้วยห้อมคอมพิวเตอร์แม่ข่าย (Server Room) ห้องผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ห้องผู้อำนวยการกลุ่มงานบริหารและบริการสารสนเทศ (เดิม) ห้องผู้อำนวยการกลุ่มงานบริหารจัดการข้อมูลข่าวสาร (เดิม) และพื้นที่ปฏิบัติงานสำหรับเจ้าหน้าที่ ประมาณ 30 คน ซึ่งประสบปัญหาความคับแคบของสถานที่ทั้งห้องคอมพิวเตอร์แม่ข่าย (Server Room) และห้องปฏิบัติงานสำหรับเจ้าหน้าที่ในสังกัดและเจ้าหน้าที่จากหน่วยงานภายนอก (Outsourcing) จึงมีความจำเป็นในการขยายพื้นที่ให้สามารถรองรับงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยขออนุมัติโครงการจัดทำห้องศูนย์ปฏิบัติการข้อมูลข่าวสารกลาง สำนักงานปลัดกระทรวงแรงงาน เพื่อให้การบริหารจัดการระบบข้อมูลของคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ให้มีประสิทธิภาพเกิดความมั่นคงปลอดภัยและมีระบบป้องกันพร้อมแก้ไขปัญหา กรณีเกิดความเสียหายรุนแรงหรือเหตุการณ์ฉุกเฉิน

จึงมีการเปลี่ยนแปลงสถานที่ดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ณ อาคารสำนักงานประกันสังคมเขตพื้นที่ 3 ชั้น 9 และทำให้**ห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย (Server Room) มีระบบป้องกันและแก้ไขปัญหากรณีเกิดเหตุการณ์ฉุกเฉินในปัจจุบัน** ประกอบด้วย

1. ระบบสำรองไฟฟ้าอย่างต่อเนื่อง (UPS)

ยี่ห้อ SOCOMEC SICON รุ่น MASTERYS MC360

คุณสมบัติ

1. เป็นระบบยูพีเอสแบบ DOUBLE CONVERSION ON-LINE TECHNOLOGY (VFI class) โดยทดสอบตามมาตรฐาน EN50091-3 / IEC 62040-3 ควบคุมการทำงานด้วยไมโครโปรเซสเซอร์ (FULL MICROPROCESSOR CONTROL)

2. เป็นระบบสำรองไฟฟ้าอย่างต่อเนื่อง (UPS: Uninterruptible Power Supply) ขนาดพิกัดกำลัง 60 KVA Load Power Factor 0.8 จำนวน 1 เครื่อง พร้อมระบบแบตเตอรี่สำรองไฟฟ้าในแต่ละระบบได้นานไม่น้อยกว่า 15 นาที ที่โหลดเต็มพิกัด สำหรับระบบแรงดันไฟฟ้าขาเข้า 3 Phase (3x380/400/415V, 50Hz) และระบบแรงดันไฟฟ้าขาออก 3 Phase (3x380/400/415V, 50Hz)

3. ระบบยูพีเอสสามารถต่อขยายเพิ่มเติมในอนาคตได้ ในลักษณะ PARALLEL

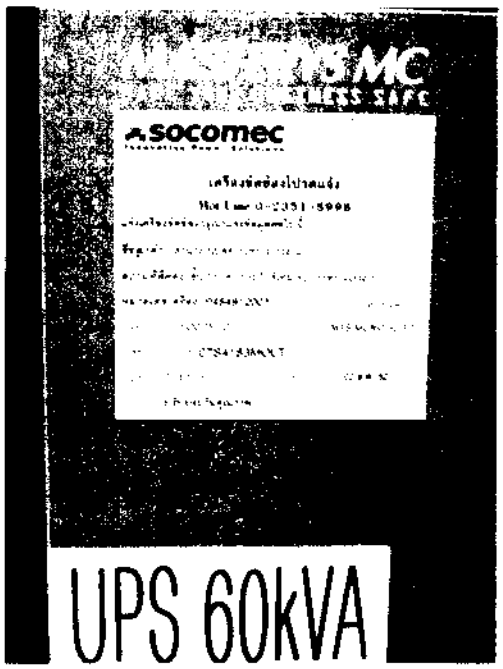
คุณสมบัติทางด้านเทคนิค

1. คุณสมบัติด้านเข้า

Input voltage	:	3 x 400 V +/- 20%
Input frequency	:	50 Hz +/- 10%
Power Factor	:	> 0.99

2. คุณสมบัติด้านขาออก

Output voltage	:	3 x 380 V +/- 1%
Rated frequency	:	50 Hz +/- 0.1%
Power rating	:	60 kVA
Load power factor	:	0.8
Voltage distortion	:	1% (linear load)
Overload	:	125% for 10 mins
		150% for 1 min
Crest Factor	:	3 : 1
Overall Efficiency	:	Up to 92%



การทำงาน

1. Normal Mode

เมื่อมีกระแสไฟฟ้าจ่ายให้ระบบยูพีเอสตามปกติ (จากระบบไฟฟ้าหลักหรือเครื่องกำเนิดไฟฟ้า) ส่วนเรียงกระแส (Rectifier) ต้องทำหน้าที่แปลงกระแสไฟฟ้าที่จ่ายเข้ามาจากแหล่งจ่ายไฟฟ้าหลัก โดยทำหน้าที่แปลงไฟฟ้ากระแสสลับให้เป็นไฟฟ้ากระแสตรงที่มีเสถียรภาพ เพื่อจ่ายให้กับส่วนอินเวอร์เตอร์ (Inverter) และอัดประจุไฟฟ้าให้แบตเตอรี่ โดยโหลดต้องได้รับพลังงานจากส่วนอินเวอร์เตอร์ (Inverter) ยกเว้นในช่วงสภาวะลัดผ่าน (Bypass Mode) เท่านั้น

2. Emergency Mode

เมื่อระบบไฟฟ้าหลักขัดข้อง โหลดทั้งหมดต้องได้รับพลังงานไฟฟ้าอย่างต่อเนื่องจากระบบแบตเตอรี่โดยปราศจากการหยุดชะงักโดยสามารถทำงานได้ตามเวลาที่กำหนดไว้ข้างต้น ในกรณีที่ระบบไฟฟ้าหลักกลับมาสู่สภาวะปกติอีกครั้ง ส่วนเรียงกระแส (Rectifier) ต้องกลับมาทำงานเองโดยอัตโนมัติเพื่อจ่ายไฟฟ้าให้กับส่วนอินเวอร์เตอร์ (Inverter) และทำหน้าที่อัดประจุไฟฟ้ากลับให้กับแบตเตอรี่อีกครั้ง

3. Bypass Mode

3.1 Automatic Bypass

กรณีที่ยูพีเอสทำงานผิดปกติ อันเนื่องจากการใช้งานในสภาวะเกินพิกัด หรือระบบยูพีเอสขัดข้อง ระบบต้องสามารถทำหน้าที่โอนย้ายโหลดจากส่วนอินเวอร์เตอร์ ไปรับพลังงานจากชุด Static bypass switch ได้โดยไม่ทำให้เกิดการหยุดชะงัก และกรณีที่ระบบกลับมาอยู่ในช่วงที่ยอมรับได้ ชุด Static bypass switch ดังกล่าวต้องโอนย้ายกลับมา โดยอัตโนมัติโดยไม่ให้เกิดการหยุดชะงัก เช่นกัน

3.2 การลัดผ่านด้วยมือ (Manual Bypass)

ระบบยูพีเอสต้องมีสวิตช์ลัดผ่านด้วยมือใช้สำหรับงานซ่อมบำรุงและงานบำรุงรักษา และจะต้องมีระบบBack Feed Protection เพื่อป้องกันความเสียหายของ Inverter

3.3 แบตเตอรี่

แบตเตอรี่เป็นแบตเตอรี่ชนิด Maintenance Free แบบ Valve Regulate Lead Acid หรือ Sealed Lead Acid โดยสามารถสำรองไฟฟ้าในแต่ละระบบได้ไม่น้อยกว่า 15 นาที ที่ 100% LOAD และเป็นแบบ AGM (Absorb Glass Mat) Technology ได้รับการรับรองจากมาตรฐาน มอก. 718-2530 พร้อมแสดงรายละเอียดการคำนวณประกอบโดยใช้ค่า Load Power Factor 0.8 lag , End Voltage 1.70 V./C ชุดแบตเตอรี่ติดตั้งบน Rack หรือตู้ ที่แข็งแรง ซึ่งทาด้วยสีกันสนิม พร้อมทั้งชุดป้องกันการลัดวงจรของชุดแบตเตอรี่

3.4 อุปกรณ์ควบคุมและแสดงผล

อุปกรณ์ควบคุมและแสดงผลแบบ LCD Display พร้อม LED Display หรือดีกว่า สำหรับแสดงสภาวะการทำงานและสภาวะผิดปกติของ UPS มี Port รองรับการเชื่อมต่อกับคอมพิวเตอร์ สามารถเชื่อมต่อกับระบบแจ้งเตือนอัตโนมัติได้

2. เครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน (Generator)

ยี่ห้อ Power Link รุ่น GM 200C (225 kVA, Standby rate)

คุณสมบัติ

เป็นชุดเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉินชนิดติดตั้งภายนอกอาคาร พร้อมชุดตู้ครอบเก็บเสียง ใช้สำหรับจ่ายกระแสไฟฟ้าฉุกเฉินให้กับห้องศูนย์ปฏิบัติการข้อมูลข่าวสารกลาง ขนาดกำลังไฟฟ้า 225 kVA ที่ 400/230 V 3 phase 4 wire 50 Hz, power factor 0.8 กรณีมีน้ำมันเต็มถัง สามารถทำให้เครื่องกำเนิดไฟฟ้าสำรองฉุกเฉินจ่ายโหลดเต็มพิกัดได้ไม่น้อยกว่า 8 ชั่วโมง

1.เครื่องยนต์ต้นกำลัง (Engine)

1.1 เป็นเครื่องยนต์ 6 สูบ 4 จังหวะแบบล่าสุดจากโรงงานผู้ผลิต ใช้น้ำมันดีเซลเป็นเชื้อเพลิง ระบายความร้อนด้วยน้ำ ทำงานที่ Rated Speed 1500 รอบต่อนาที

1.2 ขนาดกำลังของเครื่องยนต์จะต้องเป็นขนาดที่เหมาะสมกับการใช้งานตามมาตรฐาน BS, DIN, ISO, SAE หรือมาตรฐานอื่นที่เทียบเท่า

1.3 ระบบควบคุมความเร็วรอบของเครื่องยนต์ใช้ Governor แบบ Electronic โดยควบคุมความเร็วเปลี่ยนแปลงไม่เกิน 0.5% ของ Rated Speed ที่สถานะคงตัว (Steady State)

1.4 ระบบระบายความร้อน เป็นระบบระบายความร้อนโดยใช้ Water Pump ส่งน้ำไประบายความร้อนในส่วนต่าง ๆ ซึ่งประกอบด้วย หม้อน้ำ พัดลม และ Thermostat Valve เพื่อช่วยในการควบคุมอุณหภูมิของเครื่องยนต์ให้อยู่ในสภาวะคงที่ตามที่ผู้ผลิตแนะนำ การระบายความร้อนของน้ำ ใช้ Radiator และ Blower Fan ซึ่งติดตั้งกับเครื่องยนต์ พร้อมทั้ง Guard ป้องกันส่วนเคลื่อนไหว

1.5 ระบบสตาร์ตเครื่องยนต์ใช้มอเตอร์สตาร์ตกระแสตรง พร้อมแบตเตอรี่ชนิดกรดกำมะถัน-ตะกั่ว (Sealed Lead Acid Type) หรือดีกว่า แบตเตอรี่ต้องมีความจุพอที่จะใช้สตาร์ตเครื่องยนต์ได้อย่างน้อย 5 ครั้ง มี Automatic Battery Charger

1.6 ระบบหล่อลื่นเครื่องยนต์ต้องมีเครื่องกรองน้ำมันหล่อลื่น ติดตั้งไว้ในที่บำรุงรักษาได้สะดวก

1.7 มีไส้กรองอากาศแบบ Dry Type สามารถเปลี่ยนไส้กรองอากาศได้

1.8 ระบบเชื้อเพลิง ในระบบต้องมีเครื่องกรองน้ำมันเชื้อเพลิงแบบเปลี่ยนไส้ได้ ติดตั้งในตำแหน่งที่เข้าบำรุงรักษาได้สะดวก ต้องมีอุปกรณ์สำหรับกันน้ำที่อาจจะปนอยู่ในน้ำมันเชื้อเพลิง

1.9 การลดเสียงจากท่อไอเสีย ให้มี Exhaust Silencer พร้อมทั้งมี Flexible Exhaust Pipe ข้อต่อโค้ง และอุปกรณ์ประกอบต้องประกอบสำเร็จรูปจัดวางอยู่ในชุดตู้ครอบเก็บเสียง

1.10 ระบบป้องกันเครื่องยนต์ สำหรับป้องกันการทำงานผิดปกติของเครื่องยนต์และดับเครื่องยนต์โดยอัตโนมัติ พร้อมทั้งมีไฟสัญญาณเตือนอย่างน้อยที่สุดในกรณีต่อไปนี้

1.10.1 ความเร็วรอบของเครื่องยนต์สูงเกินกำหนด

1.10.2 ความดันน้ำมันหล่อลื่นต่ำเกินกำหนด

1.10.3 อุณหภูมิน้ำหล่อเย็นเครื่องยนต์สูงเกินกำหนด

1.10.4 เครื่องยนต์สตาร์ตไม่ติด

1.11 มาตรวัดต่าง ๆ ของเครื่องยนต์ ประกอบด้วยรายการต่าง ๆ อย่างน้อยดังนี้

11.1 มาตรวัดอุณหภูมิน้ำหล่อเย็น

11.2 มาตรวัดความดันน้ำมันหล่อลื่น

11.3 มาตรวัดความเร็วรอบ

11.4 มาตรวัดชั่วโมงการทำงานของเครื่องยนต์

11.5 มาตรวัดไฟประจุแบตเตอรี่

2. <u>เครื่องกำเนิดไฟฟ้า (Alternator)</u>

2.1 เป็นแบบไม่มีแปรงถ่าน (Brushless) ต่อโดยตรงเข้ากับเครื่องยนต์ โดยผ่าน Flexible Laminated Steel Disk หรือวิธีอื่นที่ผู้ผลิตแนะนำ ออกแบบให้ระบายความร้อนด้วยพัดลมซึ่งติดบนแกนเดียวกันกับโรเตอร์

2.2 สามารถจ่ายไฟฟ้ากระแสสลับ 380/220 V 3 เฟส 4 สาย 50 Hz Power Factor 0.8 ที่ความเร็วรอบ 1500 รอบต่อนาทีโดยมีขนาด kW (หรือ kVA)

2.3 ฉนวนของขดลวดโรเตอร์และสเตเตอร์ ต้องได้ตามมาตรฐานของ NEMA Class H

2.4 การควบคุมแรงดัน (Voltage Regulator) ใช้ระบบ Automatic Voltage Regulator โดยต้องสามารถควบคุมแรงดันที่เปลี่ยนแปลงต้องไม่เกิน $\pm$ 0.5 % ที่สถานะคงตัว (Steady State)

2.5 Excitation System เป็นแบบ Self Exciter หรือ Permanent Magnet Excited Generator

3. <u>ถังน้ำมันเชื้อเพลิง (Fuel Day Tank)</u>

เครื่องกำเนิดไฟฟ้าสำรองฉุกเฉินต้องมีถังน้ำมันเชื้อเพลิงอยู่ที่แท่นฐานของเครื่อง (Sub Base Tank) มีขนาดความจุมากพอที่จะทำให้เครื่องกำเนิดไฟฟ้าสำรองฉุกเฉินจ่ายโหลดเต็มพิกัดได้ไม่น้อยกว่า 8 ชั่วโมง

4. <u>ชุดตู้ครอบกันเสียง</u>

1.เป็นชุดตู้ครอบกันน้ำ (Fully Weatherproof Enclosure) ประกอบสำเร็จจากโรงงาน ออกแบบสำหรับใช้ติดตั้งภายนอกอาคารโดยเฉพาะ

2.เป็นชุดตู้ครอบที่มีระบบการดูดซับเสียง (Sound Attenuated Enclosure) โดยมีระดับความดังของเสียงเฉลี่ยไม่เกิน 85 dB วัดที่ระยะ 1 เมตร โดยรอบตัวชุดเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน

3.เป็นชุดตู้ครอบที่ทำจากโลหะที่ผ่านกรรมวิธีการป้องกันสนิม และทนการกัดกร่อนได้ดี (Corrosion Resistant) พ่นอบสีด้วย Polyester Power Coating

การทำงาน

Automatic Starter และ Transfer Switch

1. ระบบ Automatic Starter และ Transfer Switch สามารถทำงานได้ ดังนี้

1.1 เมื่อไฟฟ้าจากการไฟฟ้าฯ ดับลงหรือไฟฟ้ามาไม่ครบทั้ง 3 เฟส หรือแรงดันไฟฟ้าจากการไฟฟ้าฯ เฟสใดเฟสหนึ่งหรือทั้ง 3 เฟส มีค่าต่ำกว่า 80% หรือค่าตามที่กำหนด (สามารถปรับตั้งค่าได้) เป็นเวลา 3 วินาที (ปรับได้ตั้งแต่ 1-10 วินาที) เครื่องยนต์จะสตาร์ตเครื่องเองโดยอัตโนมัติ

1.2 เมื่อเครื่องยนต์สตาร์ตเครื่องโดยอัตโนมัติ ในกรณีที่เครื่องยนต์สตาร์ตครั้งแรกไม่ติด ระบบสตาร์ตเครื่องยนต์จะสตาร์ตเครื่องยนต์ใหม่ติดต่อกันอีกอย่างน้อย 3 ครั้ง หากเมื่อสตาร์ตครบแล้วเครื่องยนต์ยังไม่ติด ระบบจะไม่สตาร์ตเครื่องยนต์อีกแต่จะมีสัญญาณไฟแสดงที่แผงควบคุมที่ช่อง Over Crank หลังจากตรวจแก้ไขเรียบร้อยแล้ว ให้กดปุ่ม Reset Over Crank สัญญาณไฟจะดับ ชุดสตาร์ตเครื่องยนต์อัตโนมัติจะสตาร์ตเครื่องยนต์ใหม่

1.3 เมื่อเครื่องยนต์สตาร์ตติดแล้ว เครื่องยนต์จะวิ่งตัวเปล่าจนกว่าระดับแรงดัน และความถี่ไฟฟ้ามีค่าตามพิกัด Transfer Switch จึงจะสับไฟจ่ายกระแสไฟฟ้าจากเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน

1.4 เมื่อไฟฟ้าจากการไฟฟ้าฯ มาตามปกติครบทั้ง 3 เฟส ภายใน 3 นาที (โดยปกติตั้งไว้ที่ประมาณ 3-5 นาที) Transfer Switch จะทำหน้าที่เปลี่ยนแปลงการจ่ายโหลดจากเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน เป็นการจ่ายโหลดจากการไฟฟ้าฯ แทนโดยอัตโนมัติ แต่เครื่องยนต์ยังคงวิ่งตัวเปล่าต่อไปอีกประมาณ 5 นาที จึงจะดับเครื่องยนต์เอง ในกรณีที่ไฟฟ้าจากการไฟฟ้า ฯ เกิดดับลงไปอีกในขณะที่เครื่องยนต์กำลังวิ่งตัวเปล่าอยู่ Transfer Switch จะกลับไปทำงานตามข้อ 1.3 ใหม่ทันที

2. ในสภาวะปกติ เครื่องยนต์จะต้องสามารถสตาร์ตอุ่นเครื่องได้โดยอัตโนมัติทุก ๆ 7-10 วัน ครั้งละ 15-30 นาที (สามารถปรับตั้งได้) ในช่วงระยะเวลาอุ่นเครื่องนี้จะไม่มีการจ่ายโหลดแต่อย่างใด เว้นแต่ว่าช่วงระยะเวลาอุ่นเครื่อง ไฟฟ้าของการไฟฟ้าฯ เกิดดับลง Transfer Switch จะเริ่มทำงาน ตามข้อ 1.3 ทันที

3. Automatic Transfer Switch ติดตั้งภายใน Essential Distribution Board เป็นผลิตภัณฑ์ตามมาตรฐาน IEC และผ่านการทดสอบการใช้งานจากโรงงานผู้ผลิตมาแล้ว และสามารถเปลี่ยน Mode การทำงานเป็นแบบ Manual Operation ได้

4. แผงสวิตช์สำหรับ Automatic Starter และ Automatic Transfer Switch ประกอบด้วยอุปกรณ์ดังนี้

4.1 Pilot Lamp แสดงตำแหน่งของ Transfer Switch ทั้งทางด้าน Normal Sourceและ Emergency Source

4.2 Automatic Starter Control Panel พร้อมกับ Selector Switch เพื่อเลือกโหมดการทำงานแบบ Auto, Off, Manual, Test

4.3 By Pass Switch

3. <u>เครื่องปรับอากาศแบบควบคุมความชื้น (Precision Air)</u>

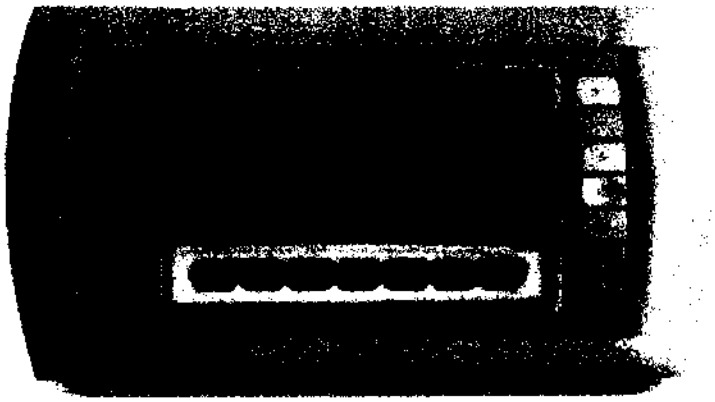
ยี่ห้อ SOCOMEC AIR CL Series รุ่น D280A /2CACR50-6

<u>คุณสมบัติ</u>

เครื่องปรับอากาศควบคุมความชื้นอัตโนมัติ ขนาดไม่น้อยกว่า 200,000 BTU/h จำนวน 2 เครื่อง ทำงาน 1 เครื่องและสำรอง 1 เครื่อง สำหรับห้อง Server Room โดยเครื่องปรับอากาศที่เสนอเป็นแบบส่งลมเย็นจากด้านล่าง (Down Flow Direction) สามารถทำความเย็น ความร้อน ลดความชื้น เพิ่มความชื้น กรองฝุ่นละอองให้สภาวะอากาศภายในห้องให้อยู่ในระดับ 22 $\pm$1^{o}C และความชื้นสัมพัทธ์ 50 $\pm$5%RH โดยเครื่องปรับอากาศทั้งชุด ได้รับมาตรฐาน ISO 9001:2000

<u>การทำงาน</u>

การทำงานของเครื่องปรับอากาศแบบควบคุมความชื้นสามารถสลับการทำงานเมื่อเครื่องปรับอากาศที่ต้องเดินเครื่อง (Duty) ใช้งานอยู่เสียหาย หรือไม่สามารถควบคุมอุณหภูมิและความชื้นภายในห้องได้ วงจรควบคุมต้องสามารถสั่งให้เครื่องปรับอากาศสำรอง (Stand-By) เดินเครื่องขึ้นมาได้โดยอัตโนมัติ และที่สภาวะปกติ ชุดควบคุมต้องสั่งให้เครื่องสำรอง (Stand-By) ทำงานสลับกับเครื่องทำ (Duty) โดยอัตโนมัติ ในกรณีที่เครื่องไม่สามารถทำงานได้เองโดยอัตโนมัติ เครื่องจะต้องสามารถทำงานได้โดยผ่านทางผู้ใช้งานหรือตามความเหมาะสมที่ผู้ใช้งานกำหนด



วิธีการใช้งานเครื่องปรับอากาศ socomec

1. กดปุ่ม ▬ เมื่อต้องการ ON เครื่อง และกดปุ่ม ▬ นี้อีกครั้งเมื่อต้องการ OFF เครื่อง
2. กดปุ่ม ▬ เลือก LEVEL1 ถ้าต้องการ SET POINT ตามด้วย PASSWORD กดปุ่ม ▬ หรือ▬ เพื่อเปลี่ยนค่า และกดปุ่ม ▬ เพื่อยืนยัน ค่าที่ต้องการ
3. เมื่อมี ALARM ให้กดปุ่ม ▬ เพื่อหยุดเสียง ALARM กดปุ่ม ▬ อีกครั้ง เพื่อ RESET ALARM กดปุ่ม▬ เพื่อเข้าสู่สภาวะการทำงานปกติ
4. กรณีมี ALARM ต่อไปนี้แล้ว RESET ไม่หายให้แจ้ง บริษัทฯ

*Airflow fail*Hp1 * Hp2 * Lp1* Lp2* Klixon Alarm
*Filter dirty *Water on floor *High Temp *Low Temp

หมายเหตุ PASSWORD = 0000

4. <u>ระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector)</u>

ยี่ห้อ Leak Sense, Aqualarm รุ่น LS-2

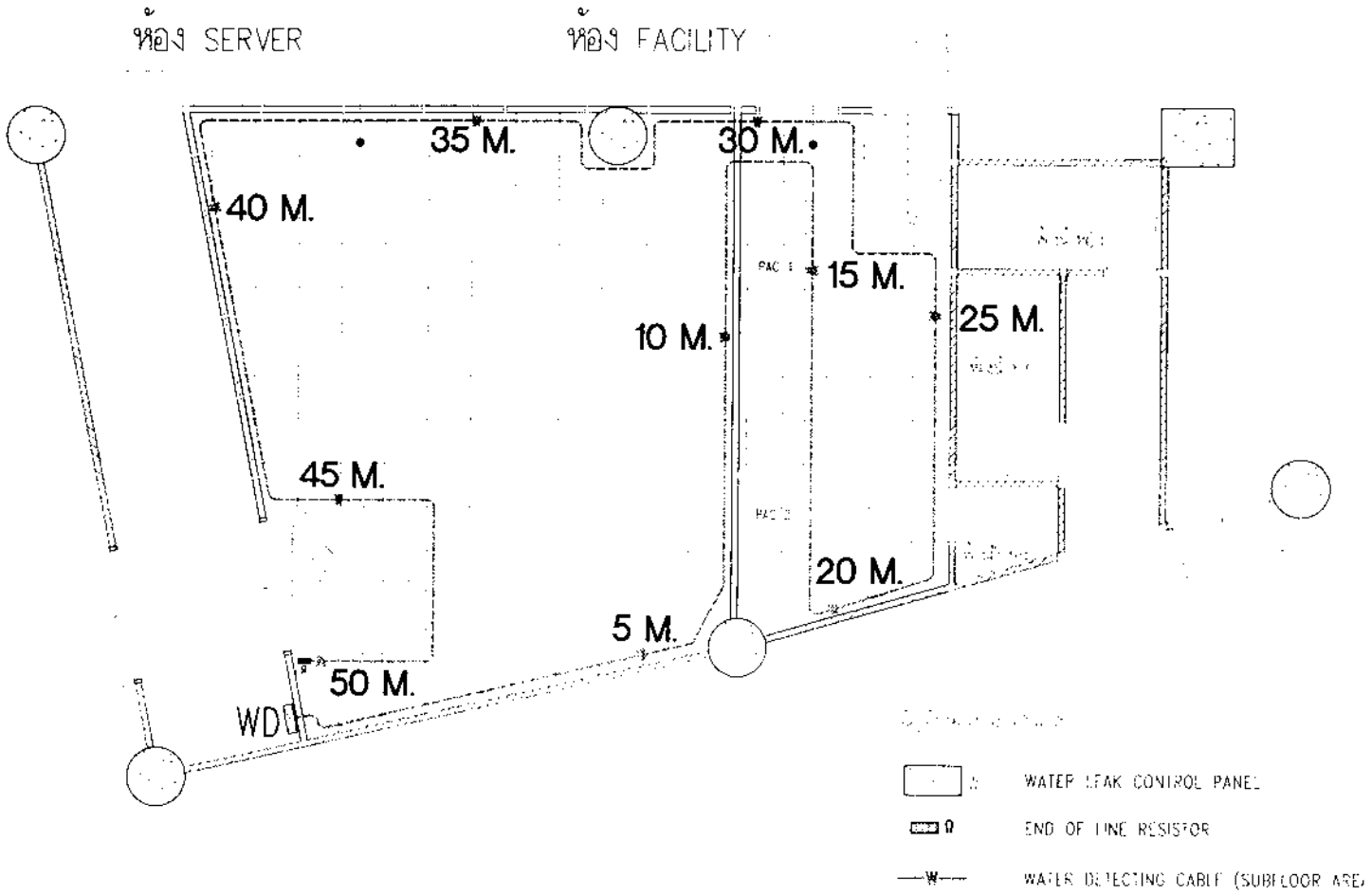
<u>คุณสมบัติ</u>

ระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector System) ชนิดตรวจจับด้วยสายเคเบิลที่ติดตั้งบริเวณใต้พื้นยกภายในห้องปฏิบัติการข้อมูลข่าวสารกลาง (Server Room) บริเวณใต้เครื่องปรับอากาศควบคุมความชื้นทุกเครื่องและบริเวณใต้ท่อน้ำภายในห้อง Server และห้อง Facility ซึ่งถือเป็นบริเวณพื้นที่สำคัญ ทั้งนี้เพื่อป้องกันการรั่วซึมของน้ำจะสามารถตรวจจับและแจ้งเตือนได้แม่นยำ โดยชุดควบคุม (Controller) มีคุณสมบัติทางเทคนิค ดังนี้ 1) สามารถตรวจจับน้ำรั่วซึมได้ไม่น้อยกว่า 500 เมตร 2) สามารถบอกระยะได้ในหน่วยเมตร ได้ 0-500 เมตร 3) มีจอแสดงผลเป็น LCD 4) มี Alarm output Contact 5) สามารถเชื่อมต่อกับระบบ BMS แบบ 4-20 mA (output) ได้ และ 6) สามารถส่งสัญญาณเชื่อมต่อไปยังระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System) และส่งข้อความ SMS นี้ไปยังโทรศัพท์เคลื่อนที่ของผู้ดูแลระบบโดยอัตโนมัติได้

<u>การทำงาน</u>

ชุดควบคุมระบบตรวจจับและแจ้งเตือนเมื่อเกิดการรั่วซึมของน้ำ (Water Leak Detector System) สามารถตรวจจับการรั่วซึมของน้ำและแจ้งระยะที่ตรวจพบการรั่วซึมของน้ำไปยัง Controller ชุดควบคุมสามารถบันทึก alarm เวลา วันที่ ที่เกิด alarm ได้

WATER LEAK DETECTION SYSTEM LAYOUT PLAN (SUBFLOOR AREA)



5. ระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environmental Monitoring System)

ยี่ห้อ PICOBOX รุ่น MESSAGE MASTER 2000

คุณสมบัติ

ระบบเฝ้าดูและแจ้งเตือนอัตโนมัติของห้องศูนย์ปฏิบัติการข้อมูลข่าวสารกลาง เมื่อเกิดความผิดปกติขึ้นจะส่งสัญญาณการแจ้งเตือนไปยังชุดควบคุมและทำการแจ้งเตือนผ่านระบบข้อความ SMS ไปยังโทรศัพท์เคลื่อนที่ของผู้ดูแลระบบโดยอัตโนมัติ และบันทึกการแจ้งเตือนไว้เพื่อสามารถนำกลับมาตรวจสอบได้

การทำงาน

1. ระบบ EMS สามารถแสดงผลและควบคุมผ่าน Web Browser interface (HTML) โดยสามารถทำการใส่ค่า IP Address ของระบบ EMS ในโปรแกรม Web Browser interface (HTML)

2. สามารถแสดงผลการทำงานผ่าน LED และ LCD Display (with Backlight)

3. สามารถส่งข้อความแจ้งเตือนผ่านระบบ SMS ไปยังโทรศัพท์เคลื่อนที่ ได้ไม่น้อยกว่า 40 หมายเลข

4. สามารถตรวจสอบสถานะความผิดปกติปัจจุบัน ผ่านระบบเครือข่ายได้

5. สามารถตรวจสอบสถานะของระบบจากโทรศัพท์มือถือผ่านระบบ SMSได้

6. รองรับการตรวจจับความผิดปกติและพร้อมส่ง Alarm Message เมื่อตรวจจับพบความผิดปกติของอุปกรณ์ต่างๆ ภายในห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ดังนี้

6.1 ระบบสำรองไฟฟ้าอัตโนมัติ

6.2 ระบบเครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น

6.3 ระบบดับเพลิงอัตโนมัติ

6.4 ระบบตรวจจับควันไฟความไวสูง

6.5 ระบบตรวจจับการรั่วซึมของน้ำ

6.6 ระบบการเข้า - ออกประตู

6.7 ระบบเครื่องกำเนิดไฟฟ้าสำรองฉุกเฉิน

6. ระบบดับเพลิงอัตโนมัติพร้อมระบบตรวจจับควันไฟความไวสูง

6.1 ระบบดับเพลิงอัตโนมัติ : Fire Suppression System ยี่ห้อ KIDDE โดยใช้สาร FM-200 (HFC227ea)

คุณสมบัติระบบดับเพลิงอัตโนมัติ

เป็นระบบดับเพลิงอัตโนมัติด้วยก๊าซ Clean Agent HFC 227ea Heptafluoropropane (CF3CHFCF3) โดยครอบคลุมถึงบริเวณพื้นที่ใช้งานภายในห้อง Server Room ,ห้อง Facility และบริเวณใต้พื้นยกของทั้งสองห้อง อุปกรณ์ของระบบเป็นไปตามมาตรฐาน UL (UNDERWRITERS LABORATORIES) และFM (FACTORY MUTUAL) และ DOT (DEPARTMENT OF TRANSPORTATION) เป็นชนิด Fixed Pipe Total Flooding System โดยกำหนดให้มีความเข้มข้นของก๊าซ HFC 227ea ไม่น้อยกว่า 7% ต่อปริมาตรห้องและไม่น้อยกว่า 7% ในพื้นที่ใต้พื้นยกที่อุณหภูมิ 70 องศาฟาเรนไฮร์และใช้เวลาในการฉีดสารจนหมดภายใน 10 วินาที เพื่อให้เกิดประสิทธิภาพในการดับเพลิงสูงสุด และไม่เกิดการเป็นพิษของสาร มีระบบอัตโนมัติป้องกันการรั่วซึมของก๊าซ (Leak From Return Process) เมื่อเกิดกรณีไฟไหม้ระบบจะทำงานอัตโนมัติ เช่น ปิดช่องลม

การทำงาน

การทำงานของระบบดับเพลิงอัตโนมัติด้วยสาร FM200 จะทำงานในลักษณะการฉีดสาร FM 200 ให้กระจายควบคุมห้องนั้น การทำงานของระบบฯ สามารถทำงานได้ทั้งแบบ Automatic และ Manual ได้ดังนี้

1. แบบ Automatic โดยใช้ Smoke Detector ติดตั้งแบบ Cross Zone โดยติดตั้ง Smoke Detector จำนวน 2 โซน ให้ตำแหน่งสลับกัน เพื่อควบคุมพื้นที่ห้องเดียวกัน เมื่อ Smoke Detector จากโซนใดโซนหนึ่งรับสัญญาณเพลิงไหม้ได้จะปรากฏเสียงสัญญาณและขั้นตอน ดังต่อไปนี้

(ก) Smoke Detector โซนแรกทำงาน (First Zone Alarm)

- หลอด Alarm LED โซนอลาร์ม ติดกระพริบ
- กระดิ่งจะดังเป็นจังหวะ
- ไฟกระพริบ (Strobe) ทำงาน

(ข) Smoke Detector โซนที่สองทำงาน (Second Zone Alarm)

- หลอด Alarm LED โซนอลาร์ม ติดกระพริบ
- กระดิ่งและไซเรนจะดังยาวต่อเนื่อง
- ระบบปรับอากาศหยุดทำงาน
- ชุดหน่วงเวลา (Delay Timer) เริ่มทำงาน (ปรับได้ 0-60 วินาที)

(ค) ก่อนแก๊สฉีดดับเพลิง (ในระหว่างที่ชุดหน่วงเวลาทำงานอยู่)

- ต้องการยกเลิกการทำงานให้โยกสวิทซ์รีเซ็ท และสวิทซ์ ISOLATE เพื่อตัดสัญญาณเปิดวาล์วหัวถังที่เครื่องคอนโทรล
- ต้องการขยายเวลาหรือยุดเวลาชั่วคราวให้กดอะบอร์ดสวิทซ์ (Abort Switch) เมื่อปล่อยมือที่กดเวลาจะนับใหม่

(ง) แก๊สถูกฉีดดับเพลิงเมื่อเวลาทำงานครบตามที่กำหนดไว้

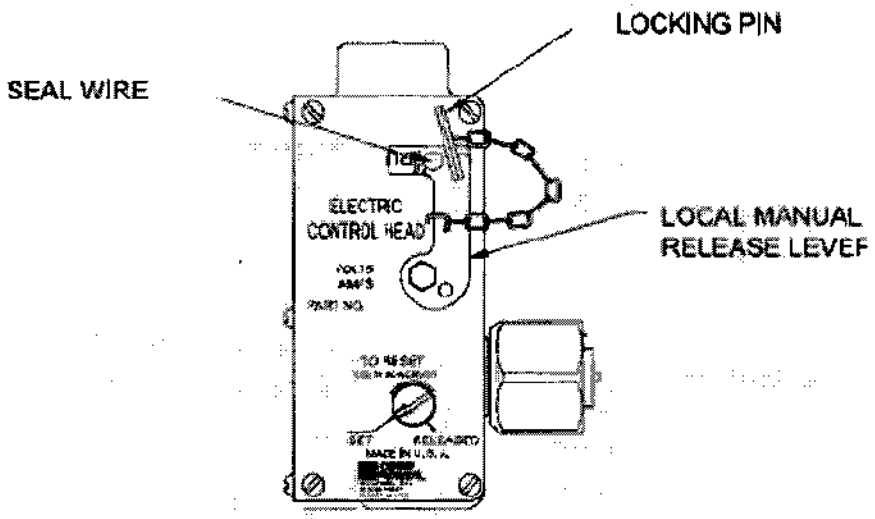
- สัญญาณจากคอนโทรลจะส่งไปชุด Solenoid ของอิเลคทริคคอนโทรลเฮด เพื่อปล่อยสลักกลไกให้เปิดวาล์วหัวถังแก๊สจะถูกฉีดออกมาเพื่อดับเพลิง
- Siren ดังยาวต่อเนื่อง (Stesdy)
- ไฟกระพริบ (Strobe) ยังคงกระพริบอยู่

2. แบบ Manual ทำได้ 2 ลักษณะ คือ

(ก) โดยการดึง Manual Pull Station ที่ติดตั้งไว้ตามจุดกำหนดไว้ช่วงเวลาใดเวลาหนึ่งจะปรากฏเสียงไซเรนดังยาวต่อเนื่อง ไฟกระพริบ (Strobe) ทำงาน แก๊สถูกฉีดออกมาดับเพลิงทันที

(ข) โดยทำการดึงสลักกลไก ซึ่งอยู่กับชุดอิเลคทริคอนโทรลเฮด (Electric Control Head) ซึ่งติดตั้งอยู่บนหัวแก๊ส FM 200 จะทำให้แก๊สถูกฉีดออกมาทันที ตัว Pressure Switch ทำงานแล้วจะส่งสัญญาณเข้าเครื่องควบคุม (Control Panel) ทำให้ไซเรน และไฟกระพริบทำงาน ซึ่งจะมีวิธีการดึงเพื่อสั่งงาน ดังนี้

วิธีการดึง Manual ที่หัวถัง
(ใช้ในกรณีฉุกเฉินเท่านั้น)



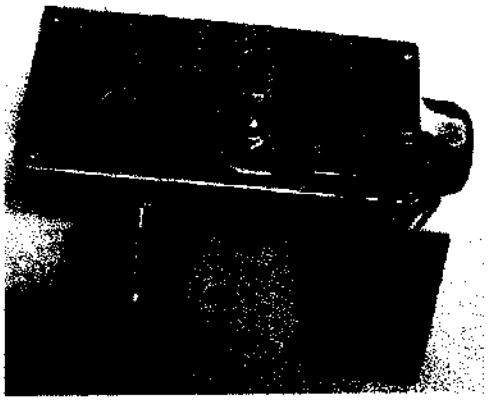
1. ดึงซีลด์ (Seal Wire) ออก
2. ดังสลักล๊อกสวิตซ์ (Locking Pin) ออก
3. โยกสวิตซ์สั่งฉีดแก๊ส (Local Manual) ขึ้น

สาร FM 200 จะถูกฉีดออกมาเพื่อดับเพลิง และ Pressure Switch ทำงานสั่งให้ระบบปรับอากาศและพัดลมระบายอากาศ หยุดทำงาน

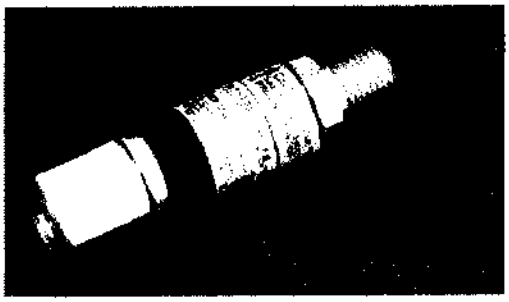
รายละเอียดอุปกรณ์ในระบบ

1. ถังบรรจุสาร FM 200 ผลิตโลหะ Steel Alloy ได้รับรองมาตรฐานจาก D.O.T., UL และ FM วาล์วหัวถังทำด้วยทองเหลืองและไม่มีชิ้นส่วนต้องเปลี่ยนใหม่ หากต้องบรรจุสารใหม่ภายหลังถูกฉีด นอกจากนี้ที่วาล์วหัวถังจะมี Pressure Gauge และ Disc Safety Device เพื่อป้องกันถังระเบิดจากแรงดันที่เพิ่มสูงขึ้น

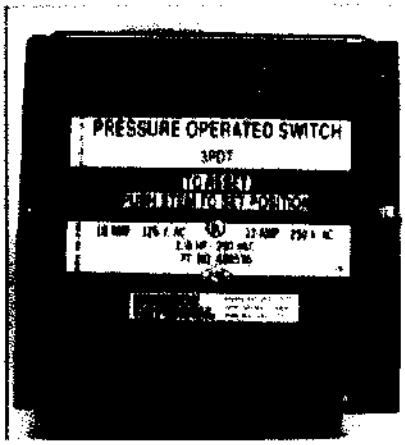
2. Electric Control Head เป็นชุด Solenoid พร้อมสลักกลไก เพื่อควบคุมวาล์วหัวถังให้ฉีดดับเพลิงเมื่อรับสัญญาณไฟฟ้าจากเครื่องคอนโทรล หรือจากการให้มือโยกก้านสลัก (Local Manual Release Lever) ที่มีซีลล็อคป้องกันการดึงเล่นและจะมีเครื่องหมายแสดงสภาวะปกติ (SET) และแสดงการถูกใช้งาน (Release)



3. Super Visory Pressure Switch ใช้สำหรับตรวจเช็คแรงดันในถังว่าลดลงต่ำกว่าอัตราปกติหรือไม่ โดยติดตั้งที่วาล์วหัวถัง ถ้าความดันลดต่ำจะส่งสัญญาณแสดงผลที่เครื่องคอนโทรล เพื่อนำถังไปซ่อมและอัดแรงดันให้อยู่ในอัตราปกติ



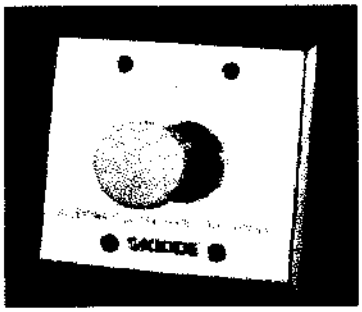
4. Pressure Operated Switch เป็นสวิทช์ที่ทำงานด้วยแรงดันของแก๊สที่ฉีดออกมาดับเพลิงภายในจะมี Contact เพื่อใช้เป็นสัญญาณส่งไปตัดการทำงานของระบบปรับอากาศ และ\หรือส่งสัญญาณกลับไปยังเครื่องคอนโทรล มีเครื่องหมายแสดงสภาวะปกติ (Set) และแสดงสภาวะการทำงาน (Operate)



5. Discharge Nozzle ทำด้วยทองเหลืองมีขนาดตั้งแต่ ½ นิ้วถึง 2 นิ้ว การเจาะรู เพื่อให้แก๊สกระจายออกมาดับเพลิงเป็นผลมาจากการคำนวณ การติดตั้งจะเป็นแบบคว่ำหัวลงเท่านั้น (Pendent)

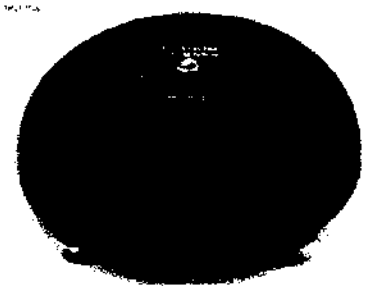
6. Manual Discharge Station ใช้สำหรับทำงานแบบแมนนวล โดยใช้มือดึงเพื่อฉีดแก๊สดับเพลิง โครงสร้างจะเป็นแบบ Double Action Operated เพื่อป้องกันอุบัติเหตุ

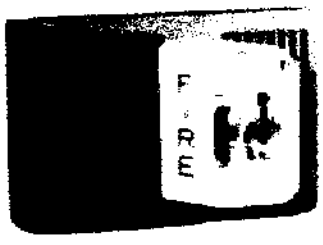
7. Abort Switch สวิทซ์มีลักษณะเป็นหัวเห็ด ใช้งานโดยการกดค้าง (Push/Hold) เพื่อยกเลิกเวลาก่อนแก๊สฉีด และเมื่อปล่อยมือเวลาจะเริ่มนับใหม่



8. Smoke Detector เป็นอุปกรณ์ตรวจจับเพลิงไหม้แบบอัตโนมัติแบบ Photoelectric การติดตั้งเพื่อใช้กับระบบดับเพลิง จะติดตั้งแบบ Cross Zone เพื่อตรวจเช็คความแน่นอนในการเกิดเพลิงไหม้ที่หัว Smoke Detector จะมีหลอด LED แสดงสภาวะการทำงาน โดยจะกระพริบในสภาวะปกติและจะติดค้างเมื่อเกิด Alarm ควบคุมพื้นที่ได้ 900 ตารางฟุตต่อ 1 หัว

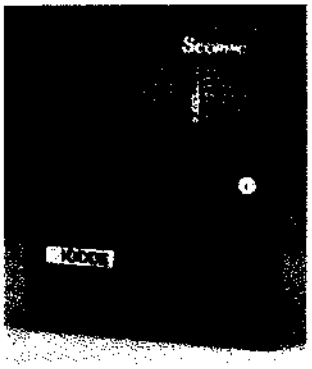
9. Bell, Siren and Strobe Lamp กระดิ่งและไซเรนเป็นแบบอิเลกทรอนิกส์ ปรับเสียงแตกต่างกันได้ 8 เสียง ส่วนไฟกระพริบมีกำลังส่องสว่าง 15/75 กำลังเทียน





Series MT Horn-Strobe

10. Control Panel



10.1 คุณสมบัติ

- ควบคุมการทำงานด้วย Microprocessor
- เป็นระบบการติดตั้งแบบ Class (2 Wires) Super Visory Line
- ออกแบบตามมาตรฐาน NFPA 72 และได้รับการอนุมัติให้ใช้ได้ระบบดับเพลิงอัตโนมัติ
- ได้รับการอนุมัติจาก UL และ FM

10.2 ฟังก์ชั่นการทำงานแบบ Cross Zone

- การตรวจจับการเกิดเพลิงไหม้แบบอัตโนมัติด้วย Smoke Detector จำนวน 2 โซน สามารถโปรแกรมให้ทำงานแบบ One Zone Alarm หรือ Two Zone Alarm (Cross Zone) ก็ได้
- เมื่อเกิด Alarm 1 โซน เสียงสัญญาณจะดังเป็นจังหวะคือ ดังยาว 1 วินาทีทุก ๆ 2 วินาที และเมื่อครบ 2 โซน สัญญาณจะดังยาวต่อเนื่อง
- เมื่อวงจรหน่วงเวลาทำงานครบมีสัญญาณส่งไปชุด Electric Control Head เพื่อสั่งการฉีดแก๊สออกจากถังเพื่อดับเพลิง
- ชุด Manual Station เพื่อสั่งการฉีดแก๊สด้วยมือ สามารถโปรแกรมให้ทำงาน โดยมีหน่วงเวลาหรือไม่มีวงจรหน่วงเวลาก็ได้
- Abort Station ใช้สำหรับหยุดเวลาของชุดหน่วงเวลาก่อนทำงานครบตามเวลาที่โปรแกรมไว้ สามารถเลือกทำงานได้ 2 แบบ
    - แบบ 1 : ขณะกดค้าง Abort Station เวลาจะนับถอยหลัง แล้วมาหยุดที่ 10 วินาที เมื่อปล่อยมือเวลาจะนับต่อจนครบ
    - แบบ 2 : ขณะกดค้าง Abort Station จะทำการ Reset เวลาที่เหลือทั้งหมดทันที เมื่อปล่อยมือเวลาจะเริ่มต้นนับใหม่
- มีวงจรหน่วงเวลา สามารถโปรแกรมปรับค่าได้ตั้งแต่ 0-60 วินาที
- ภายในมีวงจรแปลงไฟ AC220V เป็น DC 24V เพื่อจ่ายให้กับระบบ พร้อมชุดชาร์จแบตเตอรี่และแบตเตอรี่สำรอง

- มีหลอด LED แสดงสถานการณ์ทำงาน ดังนี้

หลอด	สี	แสดง
POWER ON LED	เขียว	ไฟ AC
ZONE 1 ALM LED	แดง	โซน 1 อลาร์ม
ZONE 2 ALM LED	แดง	โซน 2 อลาร์ม
MAN REL ALM LED	แดง	แมนนวลทำงาน
ABT ACT LED	เหลือง	การกดอะบอร์ดสวิทซ์
SPV ON LED	เหลือง	สัญญาณไซเรนขัดข้อง
SYS TBL LED	เหลือง	ระบบขัดข้อง
ZONE 1 TBL LED	เหลือง	โซน 1 ขัดข้อง
ZONE 2 TBL LED	เหลือง	โซน 2 ขัดข้อง
MAN REL TBL LED	เหลือง	แมนนวลสเตชั่นขัดข้อง
ABT TBL LED	เหลือง	อะบอร์ดสวิทซ์ขัดข้อง
SPV TBL LED		แรงดันในถังลดลง

- มีสวิทซ์ควบคุม ระบบ ดังนี้
  - ○ Reset Switch ใช้เพื่อปรับเครื่องสู่สภาวะปกติ
  - ○ Silence Switch ใช้เพื่อหยุดเสียงสัญญาณ Alarm และ Trouble
  - ○ Isolate Switch ใช้สำหรับเลือกสัญญาณควบคุม Electric Control Head ว่าจะให้ทำงานหรือไม่

10.3 Trouble Shooting

อาการขัดข้องของระบบต่าง ๆ จะแสดงผลด้วยสัญญาณหลอด LED และสัญญาณเสียง ดังนี้

ลำดับ	หลอด LED แสดงสถานะ	อาการขัดข้อง
1.	- หลอด AC Power สีเขียวดับ - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ - กด Silence Switch นาน 2 วินาที หลอด LED ทุกหลอดดับแล้ว หลอด AC Power สีเขียวจะติดดวงเดียว	ระบบไฟ 220 VAC ไม่จ่ายเข้าเครื่อง
2.	- หลอด Zone 1 Trouble สีเหลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สายวงจร Zone 1 ขาด
3.	- หลอด Zone 2 Trouble สีเลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สายวงจร Zone 2 ขาด
4.	- หลอด Manual Release Trouble สีเหลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สายวงจร Manual Release ขาด
5.	- หลอด Abort Trouble สีเหลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สาย Abort Switch ขาด
6.	- หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ - หลอด Supervisory On สีเหลืองจะติด หลังจากกด Silence Switch นาน 2 วินาที แล้วหลอด LED ดับทุกดวง	สายวงจร Alarm Signal ขาด
7.	- หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ - หลอด Alarm Silence สีเหลืองจะติด หลังจากกด Silence Switch นาน 2 วินาที แล้วหลอด LED ดับทุกดวง	สายวงจร Alarm Signal ลัดวงจร

ลำดับ	หลอด LED แสดงสถานะ	อาการขัดข้อง
8.	- หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ - หลอด System Trouble สีเหลืองติด หลังจากกด Silence Switch นาน 2 วินาที แล้วหลอด LED ดับทุกดวง	สายแบตเตอรี่หลุดและ/หรือแบตเตอรี่ชำรุดไม่มีกำลังไฟ
9.	- หลอด System Trouble สีเหลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สายวงจร Supervisory Pressure Switch ขาดและ/หรือแรงดันในถังลดลงต่ำกว่าเกณฑ์กำหนด
10.	- หลอด Release Output Trouble สีเหลืองติด - หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ	สายวงจร Release Output สำหรับสั่งฉีดแก๊สขาดและ/หรือ Electric Control Head บนหัวถังทำงาน
11.	- หลอด System Trouble สีเหลืองติดกระพริบ - เสียงบัซเซอร์ดังเป็นจังหวะ - หลอด Zone 1 Alarm สีแดงจะติด หลังจากกด Silence Switch นาน 2 วินาที แล้วหลอด LED ดับทุกดวง	Ground Fault สายในระบบจัดวงจรกับท่อคอนดุท

วิธีใช้เครื่องคอนโทรล ระบบดับเพลิงอัตโนมัติ

ลำดับ	หลอดไฟ	ปกติ	ทำงาน	การทำงาน
1	POWER	ติด	ติด	แสดงไฟฟ้าจ่ายในระบบ "ติดดวงเดียวแสดงระบบปกติ
2	ZONE 1	ดับ	ติด	แสดงดีเทคเตอร์ โซน 1 เกิดอลาร์มแจ้งเหตุเพลิงไหม้
3	ZONE 2	ดับ	ติด	แสดงดีเทคเตอร์ โซน 2 เกิดอลาร์มแจ้งเหตุเพลิงไหม้
3.1	หมายเหตุ			ถ้าเกิดอลาร์มพร้อมกัน 2 โซน (โซน 1 หรือ 2) สัญญาณเสียงดังเป็นจังหวะ
3.2				ถ้าเกิดอลาร์มพร้อมกัน 2 โซน (โซน 1 หรือ 2) สัญญาณเสียงดังต่อเนื่อง ระบบอัตโนมัติทำงานชุดหน่วงเวลาเริ่มนับ ถอยหลัง 60-0 วินาที ตามโปรแกรม สารดับเพลิงจะถูกฉีดออกหมดถัง
4	MAN REL	ดับ	ติด	แสดงสั่งฉีดสารดับเพลิงด้วยการดึงชุดแมนนวลสเตชั่น
5	ABORT	ดับ	ติด	แสดงชุดอบอร์ทถูกกดเพื่อหยุดเวลาระบบสั่งฉีดสารอัตโนมัติ
6	SUPV	ดับ	ติด	แสดงแรงดันในถังรั่วหรือซึมลงต่ำกว่าขีดกำหนดบัซเซอร์ดังเป็นจังหวะ
7	SIG SSIL	ดับ	ติด	กระพรอมแสดงการ กดสวิทซ์ SIG SIL เพื่อหยุดเสียง
8	SYSTEM TBL	ดับ	ติด	กระพริบแสดงระบบขัดข้อง เช่น สายขาดจะมีเสียงบัซเซอร์ดังเป็นจังหวะ
9	ZONE 1 TBL	ดับ	ติด	แสดงวงจร ดีเทคเตอร์ โซน 1 ขัดข้อง
10	ZONE 2 TBL	ดับ	ติด	แสดงวงจร ดีเทคเตอร์ โซน 2 ขัดข้อง
11	MAN REL TBL	ดับ	ติด	แสดงวงจร ชุดฉีดสารแบบแมนนวลขัดข้อง
12	ABORT TBL	ดับ	ติด	แสดงวงจร ชุดอบอร์ท เพื่อหน่วงเวลาขัดข้อง
13	SUPV TBL	ดับ	ติด	แสดงวงจรชุดวัดแรงดันในถังขัดข้อง
14	RELEASE TBL	ดับ	ติด	แสดงวงจรชุดสั่งฉีดสารดับเพลิงขัดข้อง

ลำดับ	สวิทซ์	การทำงาน
1	RESET SW.& LAMP TEST SW.	สวิทซ์รีเซ็ท กดค้าง 5 วินาที เพื่อต้องการปรับระบบสู่สภาวะปกติ หลอดจะติดทุกหลอด เมื่อปล่อยมือหลอด POWER จะติดหลอดเดียว
2	SIG SIL	สวิทซ์หยุดเสียง (SIGNAL SILENCE) กดเพื่อต้องการหยุดเสียง บัซเซอร์, กระดิ่ง ฮอร์นและหลอด SIG SIL จะติดกระพริบแทน
3	ISOLATE SW	สวิทซ์หยุดฉีดสารดับเพลิงฉุกเฉินก่อนระบบสั่งฉีด ให้โยกสวิทซ์ OFF มา ON

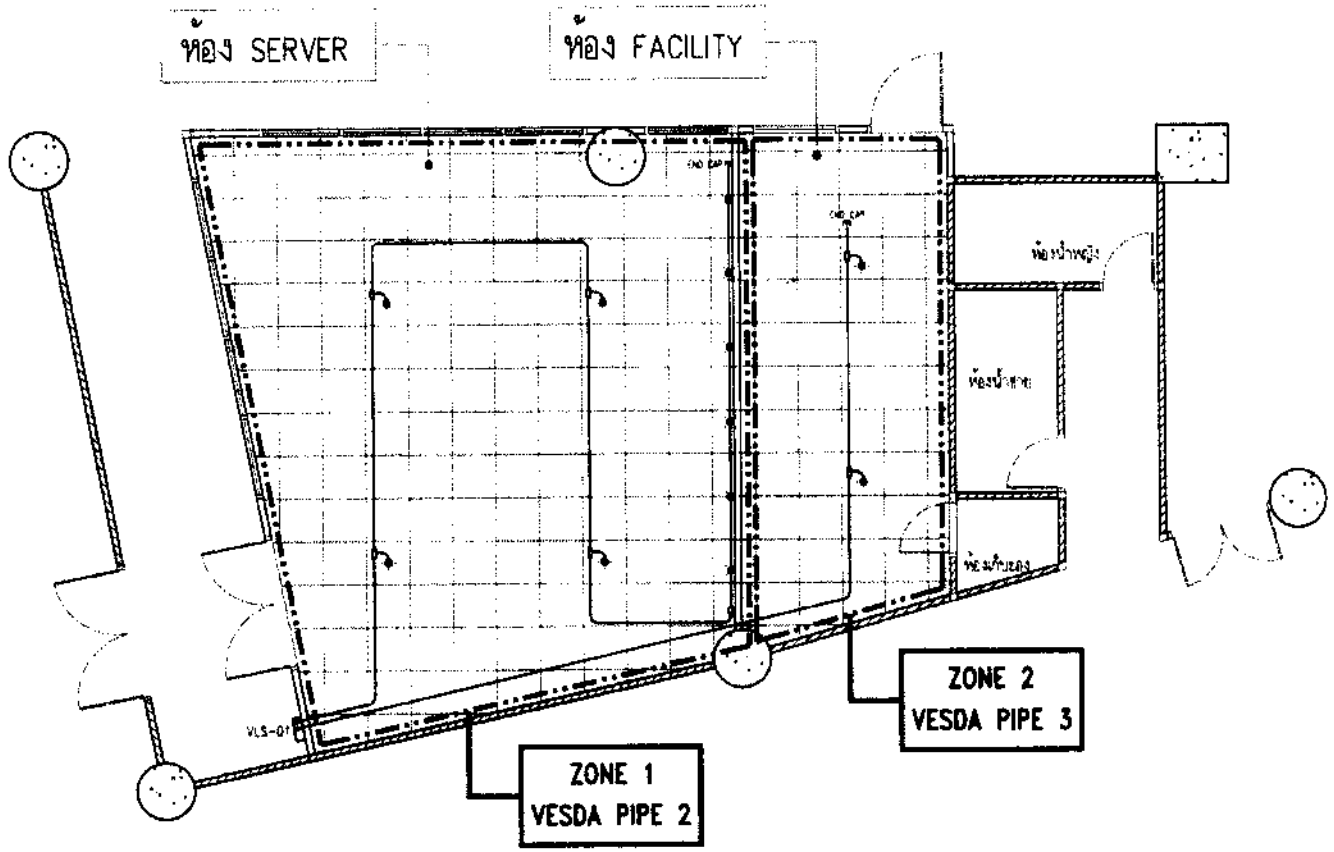
6.2 <u>ระบบตรวจจับควันไฟความไวสูง (High Senitivity Smoke Detector System</u>

ยี่ห้อ VESDA รุ่น VESDA Laser SCANNER

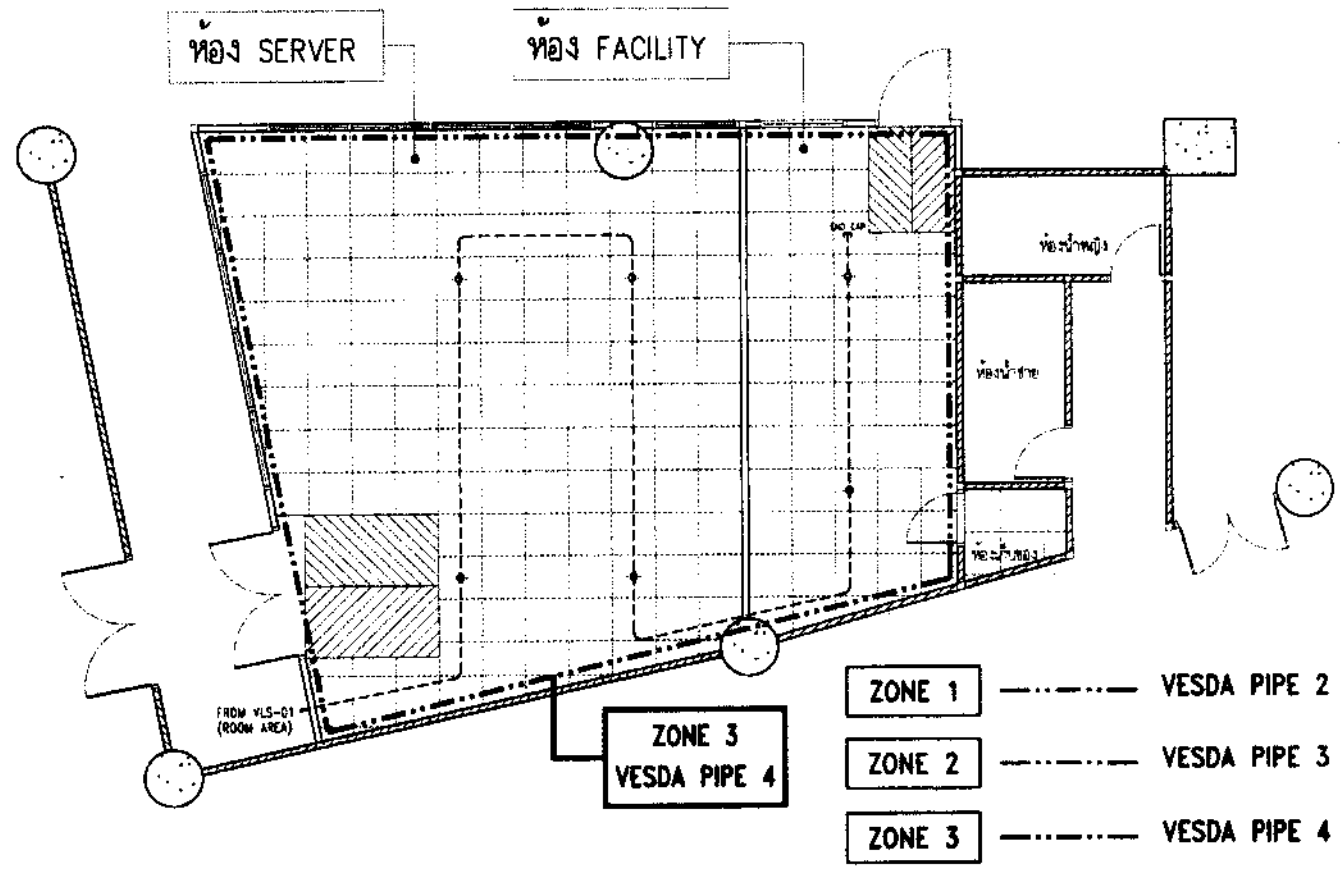
<u>คุณสมบัติ</u>

การทำงานของระบบตรวจจับควันไฟความไวสูง เป็นแบบการดูดเอาอากาศอย่างต่อเนื่อง ผ่านท่อดูดอากาศและส่งต่อไปยังส่วนตรวจจับควันด้วยเลเซอร์ (Laser detector) โดยในชุดตรวจจับควันสามารถปรับสภาพการทำงานให้เหมาะสม โดยทำการตรวจจับบริเวณเหนือช่อง Return ลม ระบบปรับอากาศควบคุมความชื้น บริเวณภายในห้อง Server (Zone 1) บริเวณภายในห้อง Facility (Zone 2) และ บริเวณใต้พื้นยกของห้อง Server และ ห้อง Facility (Zone 3)

VESDA SYSTEM LAYOUT PLAN (ROOM AREA)



VESDA SYSTEM LAYOUT PLAN (SUBFLOOR AREA)



<u>การทำงาน</u>

ระบบแจ้งเตือนเพลิงไหม้ความไวสูง (VESDA Laser SCANNER)

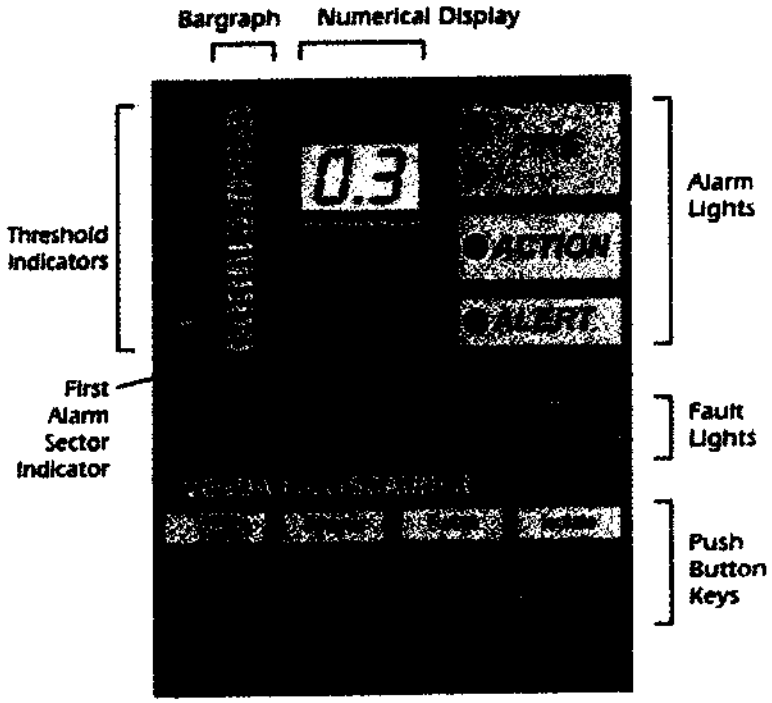
ผลิตภัณฑ์ VISION SYSTEM รุ่น VLS-304 มีพื้นที่ควบคุมเพื่อแจ้งเตือนสูงสุด จำนวน 4 โซน

ในสภาวะปกติ หลอดไฟสีเหลืองที่หน้าแผงควบคุมจะบอกตำแหน่งของระดับการตรวจจับความหนาแน่นของควันหรืออนุภาค (Threshold Indicators) มีทั้งหมด 3 ระดับ และหลอดไฟสีเขียว "OK" จะติดสว่าง พร้อมทั้งมีหลอดไฟ และ SEGMENT ของ Numerical Display แสดงให้เห็น

การแจ้งเตือนของระบบ เมื่อมีเพลิงไหม้หรือสารที่ถูกเผาไหม้เจือปนอยู่ในอากาศภายในพื้นที่ควบคุมพัดลมจะดูดอากาศ เข้ามาส่งผ่านให้ LASER DETECTOR ตรวจสอบความหนาแน่นของอนุภาคควัน โดยแสดงเป็น BARGRAPH LEVEL ตั้งแต่ 1 ถึง 10 หากพบสารใด ๆ อันเกิดจากเพลิงไหม้เจือปนอยู่ ก็จะส่งสัญญาณไปแจ้งที่ ALEART, ACTION, FIRE 1 และ FIRE 2 โดยระดับการแจ้งเตือนที่ระดับ ALERT จะส่งสัญญาณไปยัง TELE ALARM

การ RESET ระบบ เมื่อมีการแจ้งเตือนใด ๆ มาจากระบบซึ่งอาจจะเป็น FAULT หรือ ALARM โดยไม่มีเหตุขัดข้องของระบบและไม่มีสารถูกเผาไหม้เจือปนอยู่ในอากาศจริง ให้กดสวิทซ์ "RESET" เพื่อเคลียร์ระบบกลับสู่สภาพวะปกติแต่ถ้าเคลียร์ระบบกลับสู่สภาวะปกติไม่ได้ ให้กดปุ่มสวิทซ์ "ISOLATE" ที่ Push Button Keys ให้หลอดไฟสีเหลืองสว่างตรงคำว่า "ISOLATED" เพื่อให้สัญญาณแจ้งเตือน Alarm หยุดทำงานแล้วแจ้งบริษัทฯ โดยด่วน

การขัดข้องของระบบ ถ้ามีส่วนหนึ่งส่วนใดของระบบเกิดขัดข้องจะมีสัญญาณไฟโชว์ที่แผงควบคุม แสดงคำว่า "FAULT" สว่างขึ้นตามกลุ่มของ FAULT LIGHT ต่าง ๆ ของแผงควบคุมและมีเสียงบี๊บของ BUZZER ภายในเครื่องแจ้งเตือน



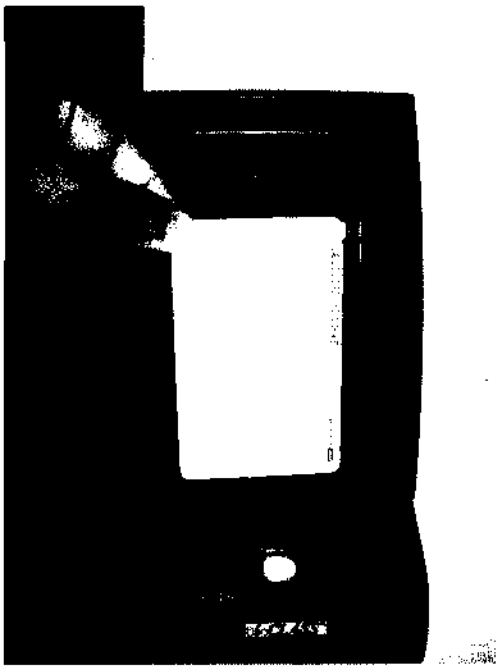
7. <u>ระบบรักษาความปลอดภัยประตูทางเข้า-ทางออก (Access Control)</u>

ยี่ห้อ BOSCH รุ่น bio CLASS RWKB575

<u>คุณสมบัติ</u>

ระบบควบคุมการเข้าออกประตูอัตโนมัติ (Access Control System) โดยติดตั้งบริเวณหน้าห้อง Server Room และ Facility Room ห้องละ 1 ชุด ซึ่งควรมีระบบรักษาความปลอดภัยทางกายภาพในการเข้าถึงคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยมีคุณสมบัติ ดังนี้

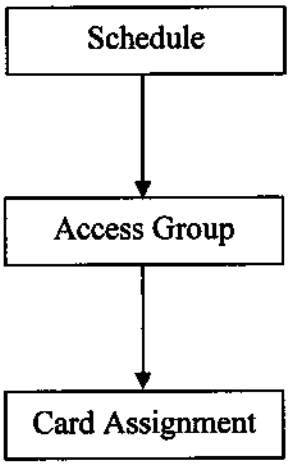
1. สามารถกำหนดกลุ่มเวลาเข้า – ออก พื้นที่ของผู้ใช้แต่ละคนได้
2. สามารถทำงานเป็นอิสระ (Stand Alone) และเก็บข้อมูล เมื่อระบบการต่อเชื่อมขัดข้อง
3. สามารถเชื่อมโยงกับเครื่องคอมพิวเตอร์เพื่อตรวจสอบเวลาการเข้า-ออกได้
4. ระบบรักษาความปลอดภัยประตูทางเข้า-ออก ประกอบด้วยอุปกรณ์ ดังนี้
   4.1 เครื่องอ่านลายนิ้วมือ Finger Print พร้อม Card Reader ติดตั้งบริเวณหน้าห้อง Server Room และห้อง Facility Room จำนวนห้องละ 3 ชุด ทั้งขาเข้าและขาออก
   4.2 กลอนประตูไฟฟ้า (Electric Door Lock) จำนวน 2 ห้อง
   4.3 จะต้องมี Proximity Card ให้จำนวน 50 ใบ



<u>การทำงาน</u>

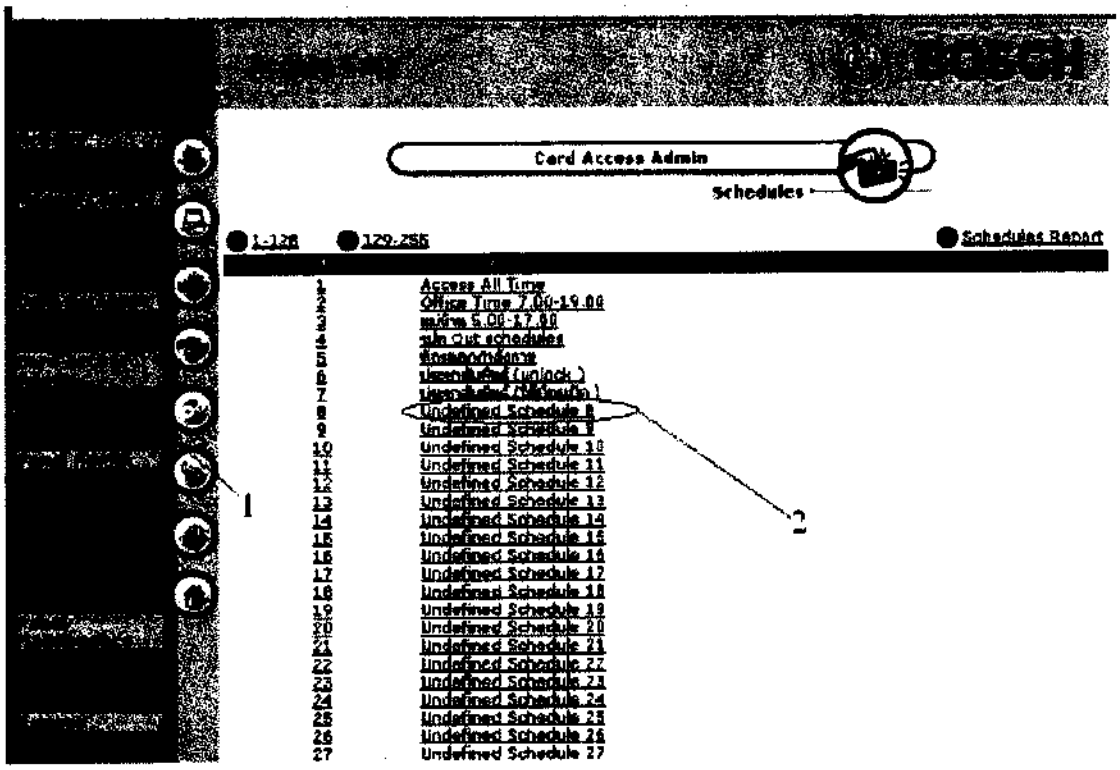
การตั้งค่าการใช้งานบัตร

1. การทำตั้งค่า Schedule เพื่อกำหนดเวลาการเข้าออกของบัตร
2. ทำการตั้งค่า Access Group เพื่อ กำหนดการเข้าออกของบัตรในแต่ละประตูโดยอ้างอิงเวลาจาก Schedule
3. ทำการตั้งค่า Card Assignment เพื่อกำหนดการใช้งานบัตร โดยอ้างอิงรูปแบบการเข้าออกจาก Access Group

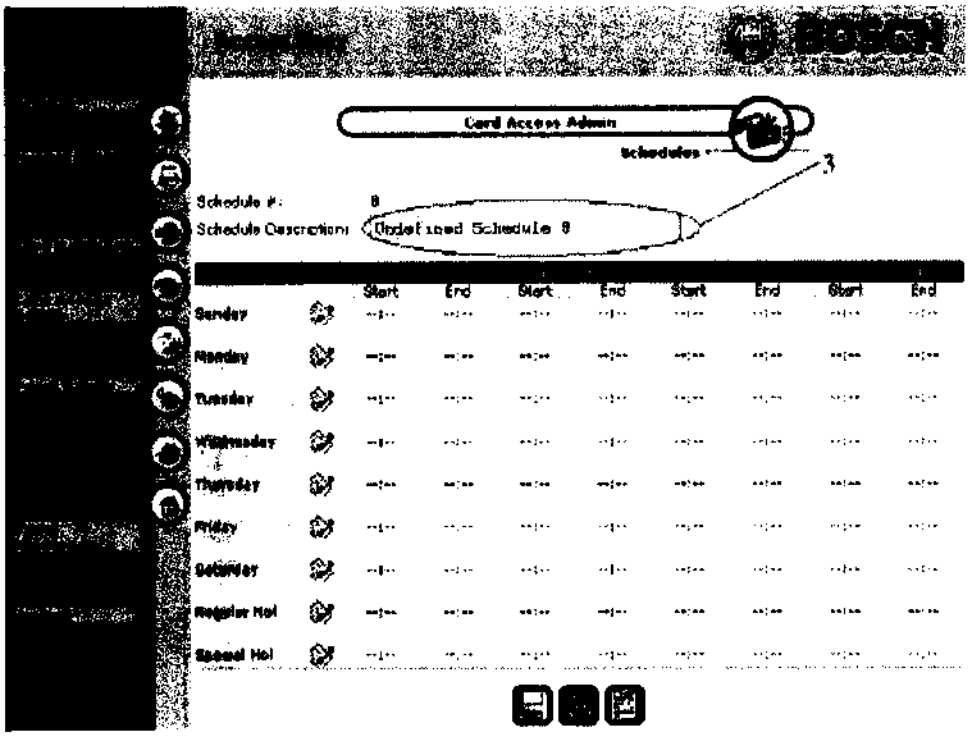


การตั้งค่า Schedule

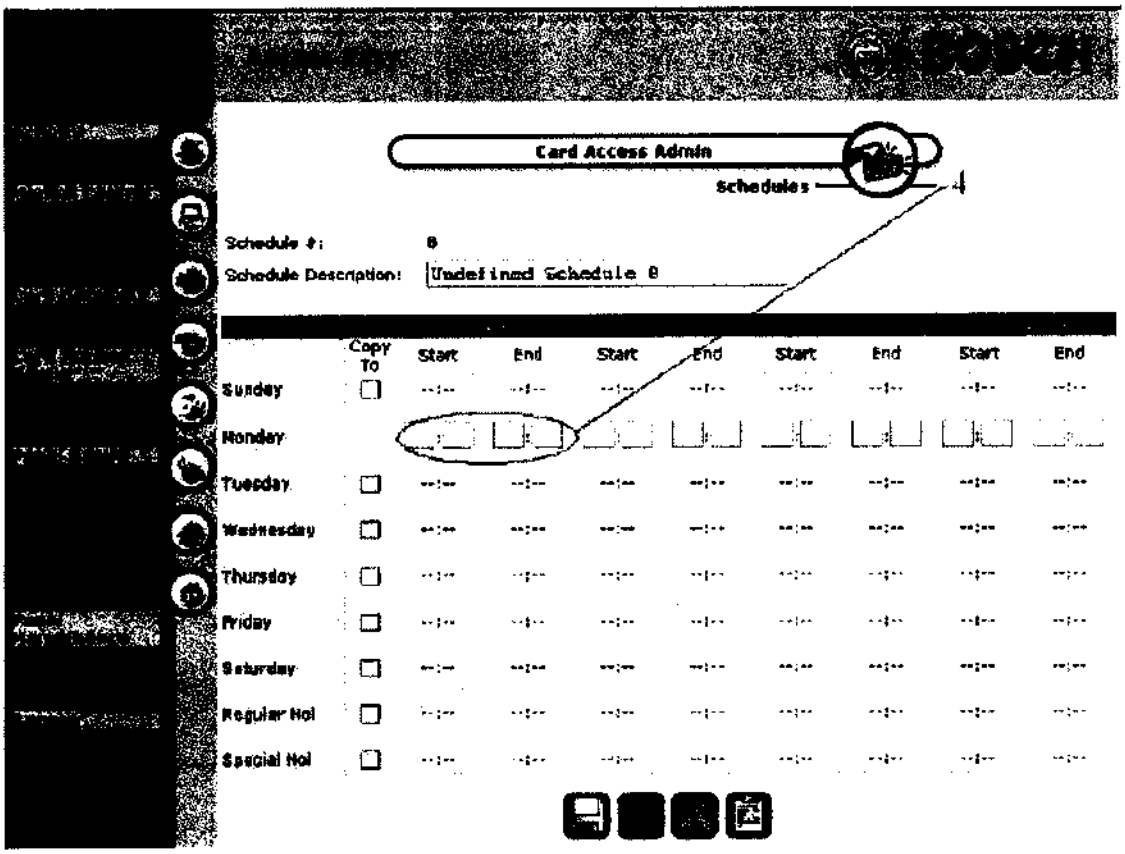
1. คลิกที่แถบ Schedule
2. คลิกที่แถบ Undefined Schedule



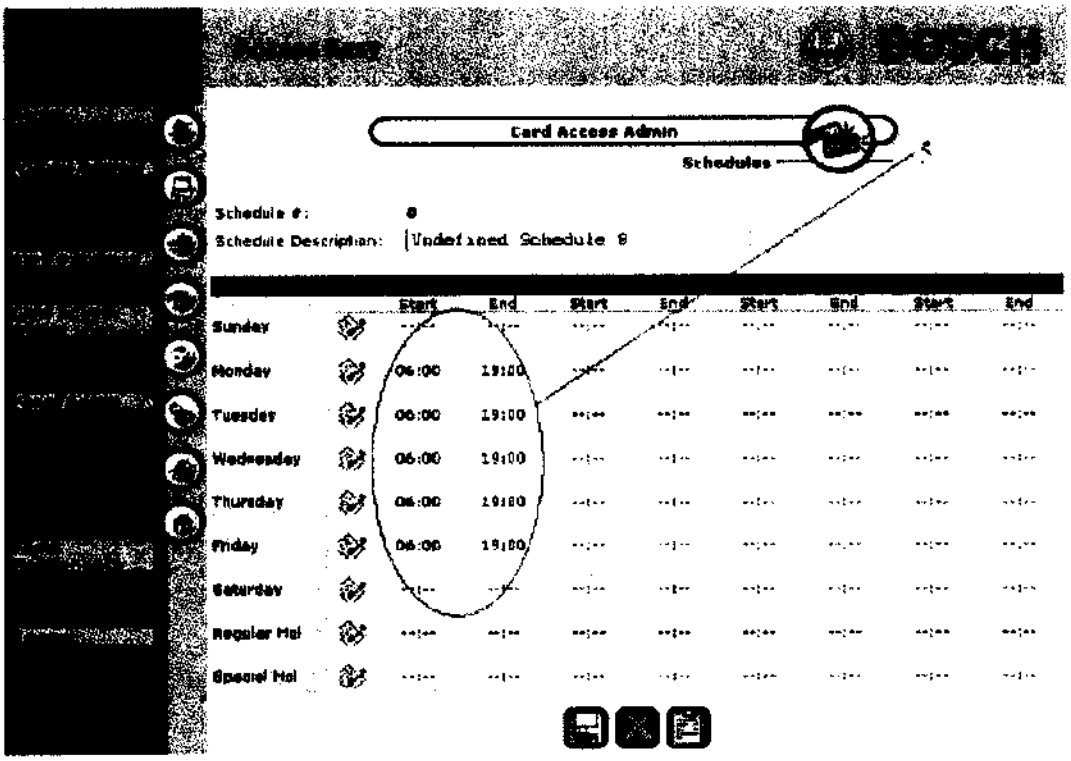
3. ทำการเปลี่ยนข้อความ Description ตามต้องการแล้วคลิก 



4. คลิก  ในวันที่ต้องการตั้งค่าเวลาการเข้าออก หลังจากนั้นทำการใส่ค่าเวลาที่ต้องการลงไปในแต่ละช่วงเวลา หากวันอื่น ๆ ใช้ค่าเวลาเหมือนกันให้คลิกในช่อง Copy To ของวันนั้น ๆ

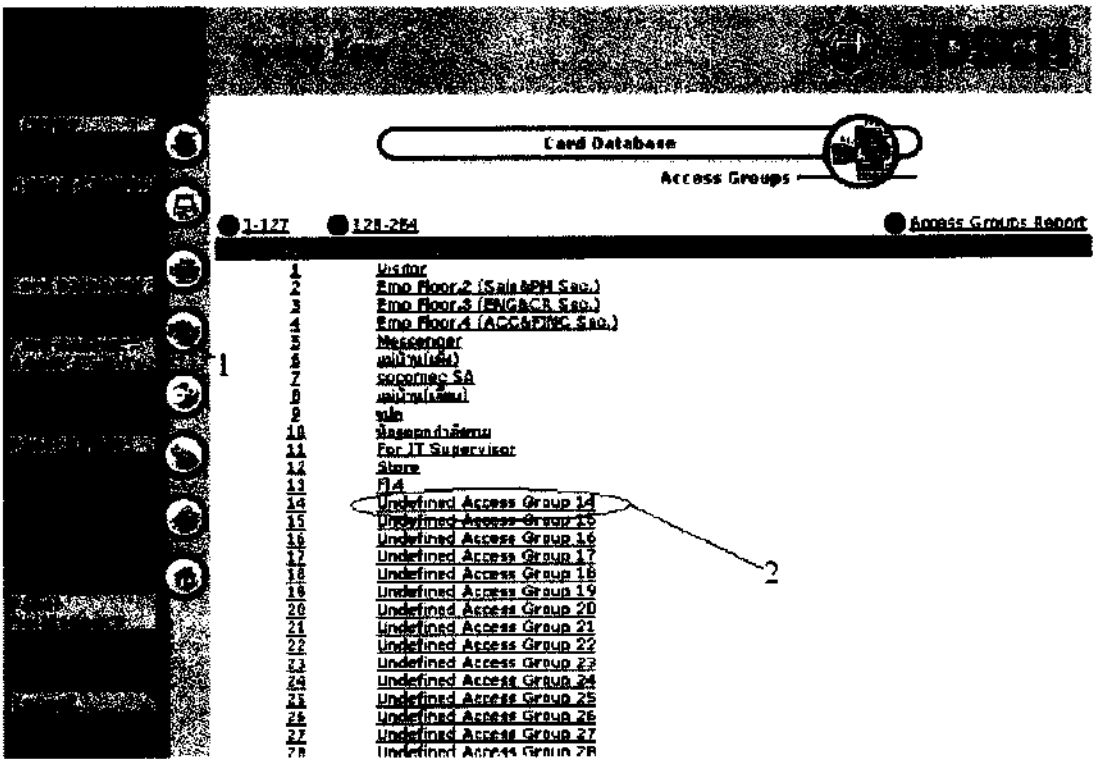


5. หลังจากนั้นคลิก  ก็จะได้ค่าเวลาการเข้าออกตามต้องการ

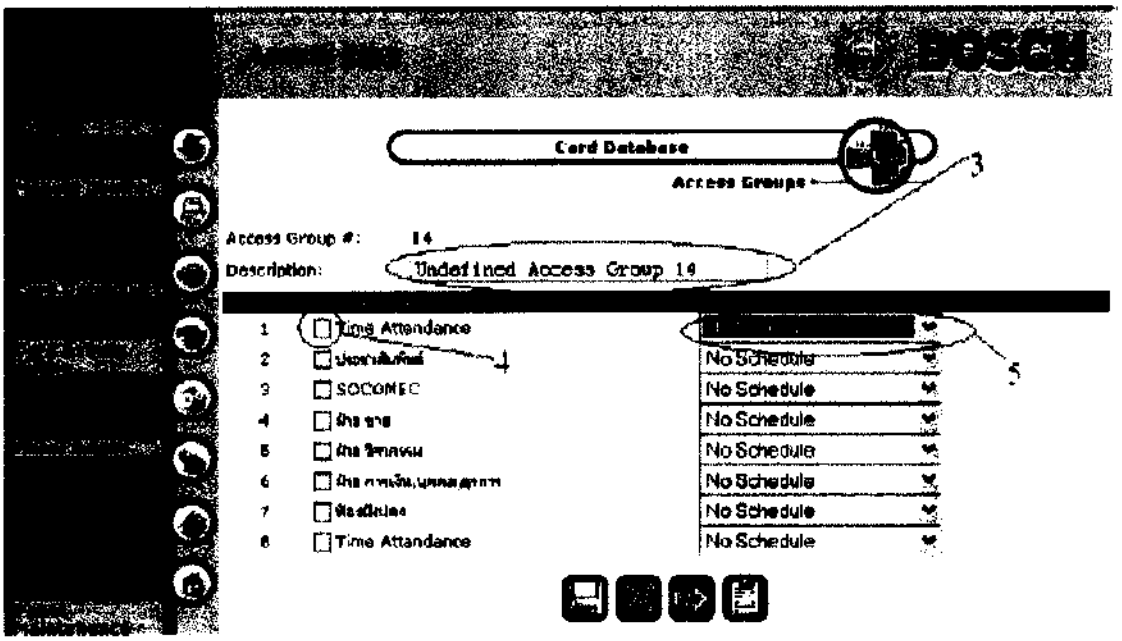


การตั้งค่า Access Group

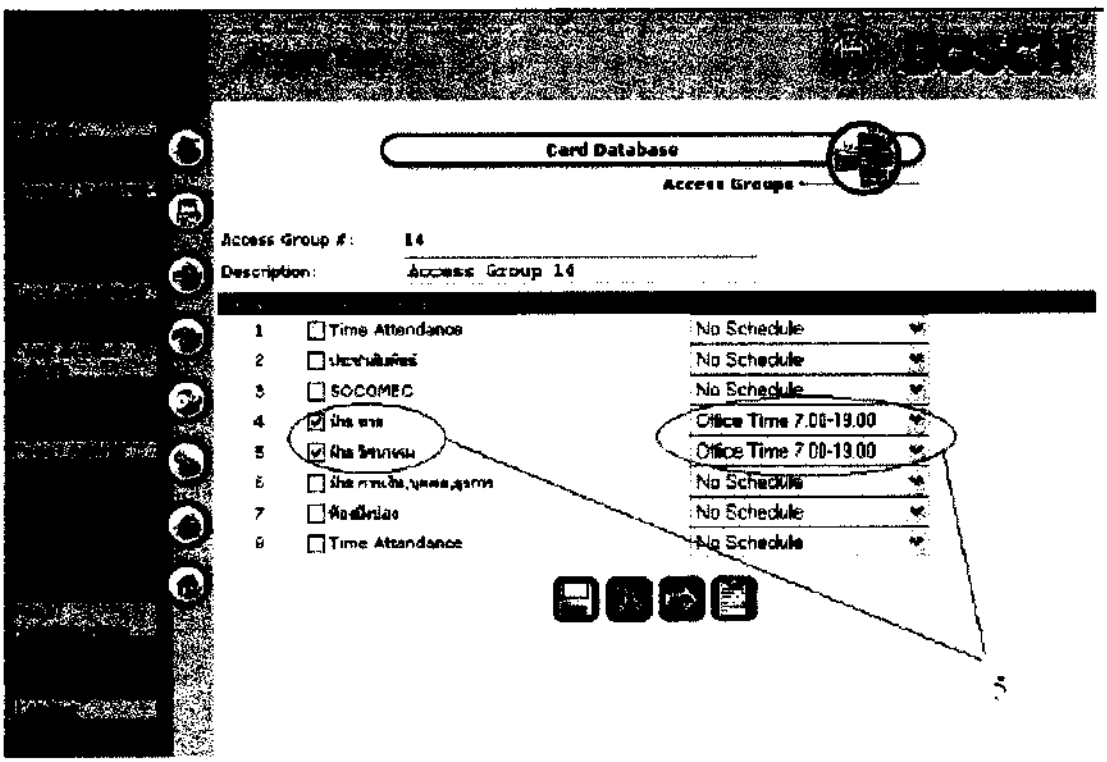
1. คลิกที่แถบ Access Group
2. คลิกที่แถบ Undefined Access Group



3. ทำการเปลี่ยนข้อความ Description ตามต้องการแล้วคลิก 
4. คลิกที่ Check Box หน้า Reader (Rdr.) ที่ต้องการกำหนดการเข้าออก
5. เปลี่ยนค่า Schedule เพื่อกำหนดเวลาการเข้าออกของ Reader นั้น ๆ ตามต้องการ



6. หลังจากนั้นคลิก  ก็จะได้ Access Group เพื่อใช้ในการกำหนดการใช้งานบัตรตามต้องการ



การตั้งค่า Card Assignment

1. คลิกที่แถบ Card Assignment
2. คลิกที่แถบ Empty Card
3. ทำการใส่ Card Number (หมายเลขบัตร) , Facility Code (หมายเลข Facility), Card Format (รูปแบบบัตร) , User Name (ชื่อผู้ถือบัตร) , Access Group (กลุ่มการใช้งานบัตร) แล้วคลิก  จึงจะสามารถใช้งานบัตรได้

รายงานการเข้า-ออก ดังนี้

All Activities Report

Thursday, 31 Jan 2008 10:07:25

Card Number : All Card Numbers
Name : All Names
Department : All Departments
Location : All Locations
Start Date : 13 Oct 2007
End Date : 31 Dec 2007
Start Time : 00:00
End Time : 23:59
1-5120 of 7029

No	Date Time	Location Card No	Activity Description User Name
1	13 Oct 2007 21:10:13	server exit ----------	Door Access Enabled ----------
2	13 Oct 2007 21:10:13	server entry ----------	Door Access Enabled ----------
3	13 Oct 2007 21:10:13	FAC exit ----------	Door Access Enabled ----------
4	13 Oct 2007 21:10:13	FAC entry ----------	Door Access Enabled ----------
5	13 Oct 2007 21:10:13	AEC Panel ----------	Panel Tampered ----------
6	13 Oct 2007 21:10:13	server exit ----------	Exit Granted ----------
7	13 Oct 2007	server entry	Exit Granted

7. <u>ระบบกล้องวงจรปิด</u>

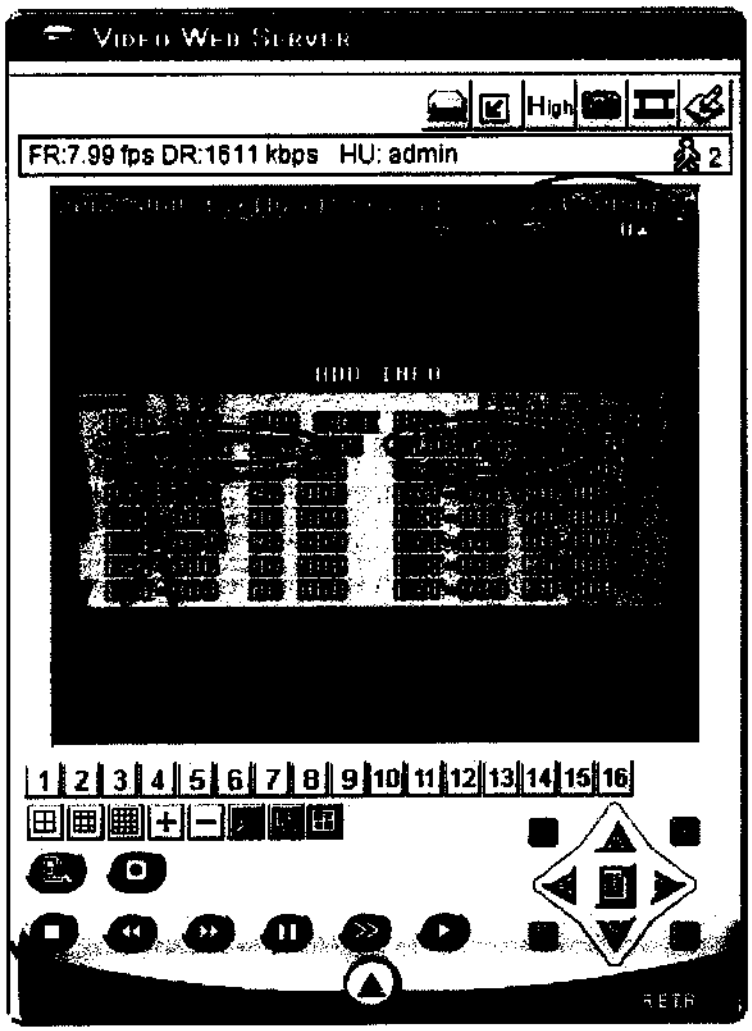
ยี่ห้อ SANYO CAMERA VCC-4795P Color CCD Camera และระบบบันทึกภาพ DVR COMPLETE AVC 787

<u>คุณสมบัติ</u>

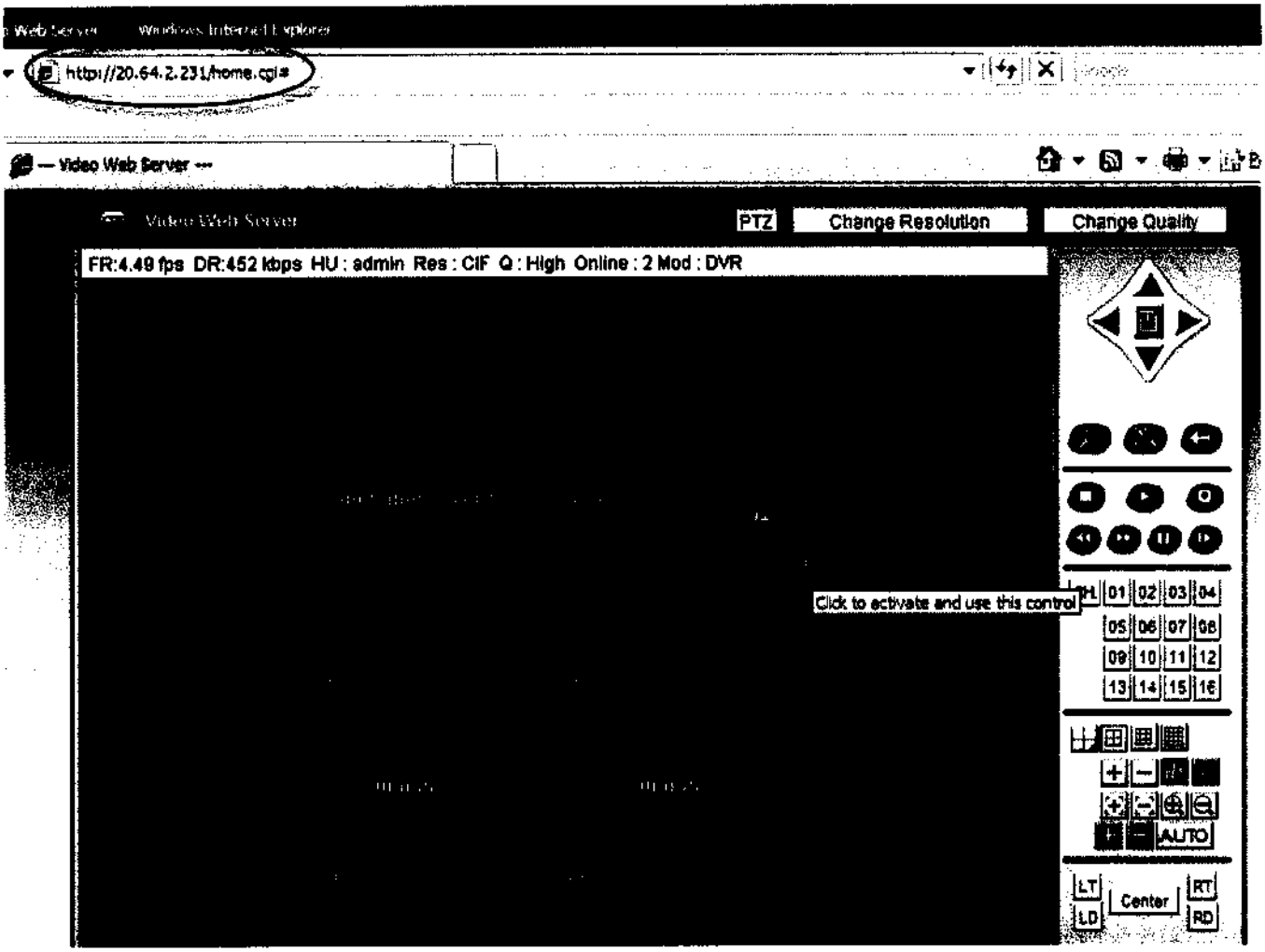
ระบบกล้องวงจรปิด (CCTV) เพื่อป้องกันควบคุม รักษาความปลอดภัยบริเวณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและหน้าห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถบันทึกภาพเหตุการณ์ที่เกิดขึ้นได้ตลอด 24 ชั่วโมง ประกอบด้วย 1) กล้องวงจรปิดชนิด Video CAM จำนวน 2 ชุด 2) ระบบบันทึกภาพ จำนวน 1 ชุด และ 3) โทรทัศน์วงจรปิด จำนวน 1 ชุด

<u>การทำงาน</u>

1.แสดงความจุของ Harddisk



2. แสดงการใช้งานแบบควบคุมจากระยะไกล



3. แสดงการตั้งเวลาการบันทึกการทำงาน