บทที่ 2
เอกสาร และงานวิจัยที่เกี่ยวข้อง

2.1 ความหมายของการพัฒนาบุคลากร

กิติมา ปรีดีดิลก (2540: 118) สรุปไว้ว่า การพัฒนากำลังคน (Manpower Development) เพื่อความมีประสิทธิภาพ ทักษะในการทำงาน เพื่อให้เกิดประสิทธิผลในการทำงาน อันจะทำให้บรรลุเป้าหมายขององค์กรได้ในที่สุด การพัฒนากำลังคนในองค์กรนั้นมีหลายวิธี แต่ที่ได้รับความนิยมกันมากที่สุดคือ การฝึกอบรม (Training) รองลงมาคือ การศึกษาต่อ และวิธีอื่น ๆ อีกมากมาย เช่น เมื่อรับบุคคลเข้าทำงานในองค์กรก็จะต้องมี การปฐมนิเทศ ซึ่งถือเป็นการพัฒนาบุคคลในขั้นแรกที่ก้าวเข้าสู่องค์กร เพื่อให้บุคคลนั้นรู้จักกับองค์กร และการทำงานในตำแหน่งที่ได้รับการบรรจุแต่งตั้ง เมื่อเข้ามาทำงานแล้วก็อาจได้รับการสับเปลี่ยนหมุนเวียนหน้าที่เพื่อจะได้รู้จักวิธีการทำงานในหน้าที่ต่าง ๆ ขององค์กร มีการสอนงาน แนะนำงาน การดูงานทั้งภายในและภายนอกองค์กร ซึ่งวิธีเหล่านี้ถือเป็นการพัฒนาบุคคลในองค์กรทั้งสิ้น

2.2 ปัจจัยที่ทำให้เกิดการพัฒนากำลังคนในองค์กร

วิจิตร อาวะกุล (2540) สรุปไว้ว่า การที่องค์กรต้องจัดให้มีการพัฒนากำลังคนขององค์กรนั้น เกิดจากปัจจัยหลายประการ กล่าวคือ

1. การเปลี่ยนแปลงขององค์กร องค์กรทุกองค์กรย่อมมีการเคลื่อนไหว และเปลี่ยนแปลงอยู่เสมอ การเปลี่ยนแปลงอาจเป็นไปในทางเสื่อมลงหรือก้าวหน้าก็ได้ ถ้าเป็นไปในทางเสื่อมลงก็จำเป็นที่จะต้องพัฒนาบุคคลให้สอดคล้องกับการเปลี่ยนแปลง คือสาเหตุของการเสื่อมโทรมเกิดจากตัวบุคคลในองค์กร ก็จะต้องฝึกอบรม และพัฒนาบุคคลในองค์กร ให้มีคุณภาพดียิ่งขึ้นเพื่อแก้ปัญหาการเสื่อมโทรมขององค์กร แต่ถ้าเปลี่ยนแปลงไปในทางก้าวหน้า เช่น องค์กรเจริญเติบโตขึ้น มีการขยายตัวขององค์กร มีการให้บริการและสินค้าเพิ่มขึ้น องค์กรจะต้องปรับโครงสร้าง และรับคนเพิ่มเพื่อให้การบริหารมีความคล่องตัว จำเป็นต้องมีการพัฒนาเทคนิคทางการบริหารของตัวผู้บริหาร มีการเลื่อนตำแหน่งที่ต้องการ การฝึกอบรมเพื่อเพิ่มทักษะในการบริหารงานให้เหมาะสมกับฐานะตำแหน่งที่เพิ่มพูนขึ้น หรือมีการรับคนใหม่ก็ต้องฝึกอบรมให้ทราบถึงวิธีการทำงาน ลักษณะของงาน และรู้จักองค์กรให้ดียิ่งขึ้น

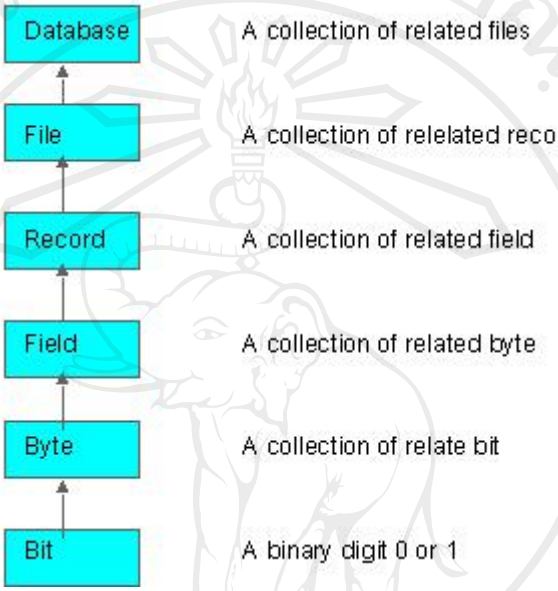
2. การเปลี่ยนแปลงทางด้านเทคโนโลยี ปัจจุบันการพัฒนาทางด้านเทคโนโลยีได้เจริญรุดหน้าไปมาก โดยเฉพาะด้านเครื่องจักรและคอมพิวเตอร์ องค์กรจึงจำเป็นต้องนำเทคโนโลยีใหม่ ๆ เข้ามาใช้เพื่อเพิ่มประสิทธิภาพขององค์กร จึงก่อให้เกิดความจำเป็นที่จะต้องพัฒนาบุคคลขององค์กรให้มีความรู้ความสามารถและทักษะ เหมาะสมที่จะปฏิบัติงานร่วมกับเครื่องจักรกลใหม่ ๆ เหล่านั้นเพื่อให้การดำเนินงานขององค์กร เป็นไปอย่างราบรื่นและมีประสิทธิภาพอย่างแท้จริง

3. สภาพแวดล้อมภายนอก คือสภาพของสังคม เศรษฐกิจ และการเมือง ซึ่งเข้ามามีผลกระทบต่อองค์กรมาก องค์กรจำเป็นที่จะต้องปรับตัวให้เข้ากับสภาพแวดล้อมเหล่านี้ เพื่อความอยู่รอดขององค์กรเอง หรือให้ได้รับความกระทบกระเทือนน้อยที่สุด เช่น เมื่อเกิดสภาพเศรษฐกิจตกต่ำ องค์กรไม่ต้องการจ้างคนเพิ่ม แต่ก็ยังจำเป็นที่จะต้องพัฒนาทางด้านเทคโนโลยี เช่น นำเอาเครื่องจักรใหม่ ๆ หรือคอมพิวเตอร์เข้ามาใช้ องค์กรจึงต้องจำเป็นที่จะใช้วิธีการฝึกอบรมบุคลากรที่มีอยู่เดิมขององค์กร ให้มีความรู้ความชำนาญเหมาะสมกับเทคโนโลยีนั้นโดยไม่ต้องรับคนเพิ่มเติม

4. พฤติกรรมของบุคคลในองค์กร พฤติกรรมหมายถึง กริยาอาการที่แสดงออก เมื่อเผชิญกับสิ่งเร้าจากภายนอก การแสดงออกนั้นอาจเกิดจากอุปนิสัยที่ได้สะสม หรือจากความเคยชินอันได้รับจากประสบการณ์ หรือการศึกษาอบรม พฤติกรรมที่แสดงออกอาจเป็นไปในทางคล้อยตามหรือต่อต้าน และอาจเป็นไปในทางที่เป็นคุณหรือโทษต่อเจ้าของพฤติกรรมเอง หรือต่อสภาพแวดล้อมและเพื่อนร่วมงานได้ โดยธรรมชาติแล้วคนมีความต้องการอยู่เสมอ และจะแสวงหาวิถีทางที่จะบรรลุความต้องการนั้น เมื่อได้รับการตอบสนองแล้วก็จะเกิดความต้องการใหม่ ๆ ขึ้นอีกอย่างไม่มีที่สิ้นสุดความต้องการของมนุษย์นี่เองที่เป็นผลให้เกิดพฤติกรรมต่าง ๆ ขึ้น สำหรับในการทำงานในองค์กรแล้ว ความต้องการของคนคือ ต้องการความมั่นคง ความพอใจในงาน โอกาสก้าวหน้าในงาน การได้รับการยกย่องนับถือ การมีผู้บังคับบัญชาที่สามารถ การได้รับค่าจ้างโดยชอบธรรม ความเสมอภาค ความต้องการเหล่านี้สามารถตอบสนองได้ และการพัฒนาบุคคลที่เป็นเครื่องมือสำคัญอันหนึ่งที่จะช่วยตอบสนองความต้องการดังกล่าวของบุคคลได้ เพราะการพัฒนาบุคคลจะช่วยให้บุคคลมีความรู้ ความชำนาญ และทัศนคติที่ดีขึ้น มีโอกาสที่จะก้าวหน้าในงาน เป็นที่ยอมรับนับถือของผู้ร่วมงานและบรรลุความต้องการต่าง ๆ ในที่สุด

2.3 Database (ฐานข้อมูล)

วิเชียร เปรมชัยสวัสดิ์ (2546) ได้ให้ความหมายของฐานข้อมูลว่า Database (ฐานข้อมูล) คือ ระบบที่รวบรวมข้อมูลไว้ในที่เดียวกัน ซึ่งประกอบไปด้วยแฟ้มข้อมูล (File) ระเบียน (Record) และเขตข้อมูล (Field) และถูกจัดการด้วยระบบเดียวกัน โปรแกรมคอมพิวเตอร์จะเข้าไปดึงข้อมูลที่ต้องการได้ อย่างรวดเร็ว ซึ่งอาจเปรียบฐานข้อมูลเสมือนเป็น electronic filing system



- บิต (bit) ย่อมาจาก Binary Digit ข้อมูลในคอมพิวเตอร์ 1 บิต จะแสดงได้ 2 สถานะ คือ 0 หรือ 1 การเก็บข้อมูลต่าง ๆ ได้จะต้องนำ บิต หลาย ๆ บิต มาเรียงต่อกัน เช่นนำ 8 บิต มาเรียงเป็น 1 ชุด เรียกว่า 1 ไบต์
- เมื่อเรานำ ไบต์ (byte) หลายๆ ไบต์ มาเรียงต่อกัน เรียกว่า เขตข้อมูล (field) เช่น Name ใช้เก็บชื่อ LastName ใช้เก็บนามสกุล เป็นต้น
- เมื่อนำเขตข้อมูล หลายๆ เขตข้อมูล มาเรียงต่อกัน เรียกว่า ระเบียน (record) เช่น ระเบียน ที่ 1 เก็บ ชื่อ นามสกุล วันเดือนปีเกิด ของ นักเรียนคนที่ 1 เป็นต้น
- การเก็บระเบียนหลายๆระเบียน รวมกัน เรียกว่า แฟ้มข้อมูล (File) เช่น แฟ้มข้อมูลนักเรียน จะเก็บ ชื่อ นามสกุล วันเดือนปีเกิด ของนักเรียน จำนวน 500 คน เป็นต้น
- การจัดเก็บ แฟ้มข้อมูล หลายๆ แฟ้มข้อมูล ไว้ภายใต้ระบบเดียวกัน เรียกว่า ฐานข้อมูล หรือ Database เช่น เก็บ แฟ้มข้อมูล นักเรียน อาจารย์ วิชาที่เปิดสอน เป็นต้น

การเข้าถึงข้อมูลในฐานข้อมูลจึงจำเป็นต้องมีระบบการจัดการฐานข้อมูลมาช่วยเรียกว่า database management system (DBMS) ซึ่งจะช่วยให้ผู้ใช้สามารถจัดการกับข้อมูล ตามความต้องการได้ ในหน่วยงานใหญ่ ๆ อาจมีฐานข้อมูลมากกว่า 1 ฐานข้อมูลเช่น ฐานข้อมูลบุคลากร ฐานข้อมูลลูกค้า ฐานข้อมูลสินค้า เป็นต้น

กิตติ ภักดีวัฒนะกุล และ จำลอง ครูอุตสาหะ (2546) กล่าวถึง ปัญหาต่างๆ ที่เกิดขึ้นในระบบแฟ้มข้อมูลว่าได้ก่อให้เกิดการจัดเก็บข้อมูลในรูปแบบใหม่ขึ้นที่เรียกว่า “ฐานข้อมูล Database” การจัดเก็บข้อมูลในฐานข้อมูลนี้จะแตกต่างจากการจัดเก็บข้อมูลแบบแฟ้มข้อมูล เนื่องจากฐานข้อมูลเป็นการนำเอาข้อมูลต่างๆ ที่มีความสัมพันธ์กัน ซึ่งแต่เดิมจัดเก็บอยู่ในแต่ละแฟ้มข้อมูลมาจัดเก็บไว้ในที่เดียวกัน เช่น ข้อมูลพนักงาน สินค้าคงคลัง พนักงานขาย และลูกค้า ซึ่งแต่เดิมเก็บอยู่ในรูปของแฟ้มข้อมูลฝ่ายต่าง ๆ ได้ถูกนำมาจัดเก็บรวมกันไว้ภายในฐานข้อมูลเดียว ซึ่งเป็นฐานข้อมูลรวมของบริษัท ส่งผลให้แต่ละฝ่ายสามารถใช้ข้อมูลร่วมกันและสามารถแก้ไขปัญหาต่างๆ ที่เกิดขึ้นในระบบแฟ้มข้อมูลได้

ข้อมูลต่าง ๆ ที่ถูกจัดเก็บเป็นฐานข้อมูล นอกจากจะต้องเป็นข้อมูลที่มีความสัมพันธ์กันแล้ว ยังจะต้องเป็นข้อมูลที่ใช้สนับสนุนดำเนินงานอย่างน้อยอย่างใดอย่างหนึ่งขององค์กร ดังนั้นจึงอาจกล่าวได้ว่า แต่ละฐานข้อมูลจะเทียบเท่ากับระบบแฟ้มข้อมูล 1 ระบบ และจะเรียกฐานข้อมูลที่จัดทำขึ้นเพื่อสนับสนุนการดำเนินงานอย่างใดอย่างหนึ่งนั้นว่า “ระบบฐานข้อมูล (Database System) เช่น ระบบฐานข้อมูลเงินเดือน ซึ่งเป็นฐานข้อมูลที่จัดเก็บข้อมูลต่างๆ ที่สนับสนุนการคำนวณเงินเดือน หรือระบบฐานข้อมูลประชากร ซึ่งเป็นฐานข้อมูลที่จัดเก็บข้อมูลต่าง ๆ ที่สนับสนุนการจัดทำสำมะโนประชากร เป็นต้น”

2.4 หลักการทำงานของ PHP

ในปัจจุบัน Web site ต่าง ๆ ได้มีการพัฒนาในด้านต่างๆ อย่างรวดเร็ว อาทิเช่น เรื่องของความสวยงาม ความแปลกใหม่ การบริการข่าวสารข้อมูลที่ทันสมัย และเป็นสื่อกลางในการติดต่อสื่อสาร ความสามารถที่โดดเด่นอีกประการ-หนึ่งของ PHP นั้น คือ database-enabled web page ทำให้เอกสารของ HTML สามารถที่จะเชื่อมต่อกับระบบฐานข้อมูล (database) ได้อย่างมีประสิทธิภาพ และรวดเร็ว ตลอดจนการจัดเก็บข้อมูลต่าง ๆ ที่สำคัญผ่านทาง Internet เป็นไปได้อย่างง่ายดาย

ข้อมูลจาก www.thaicreate.com กล่าวว่า PHP เป็นภาษาจำพวก scripting language คำสั่งต่างๆจะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ (script) และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ก็เช่น JavaScript, Perl เป็นต้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบ

อื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า server-side หรือ HTML-embedded scripting language เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

เนื่องจากว่า PHP ไม่ได้เป็นส่วนหนึ่งของตัว Web Server ดังนั้นถ้าจะใช้ PHP ก็จะต้องดูก่อนว่า Web server นั้นสามารถใช้สคริปต์ PHP ได้หรือไม่ ยกตัวอย่างเช่น PHP สามารถใช้ได้กับ Apache WebServer และ Personal Web Server (PWP) สำหรับระบบปฏิบัติการ Windows 95/98/NT ในกรณีของ Apache เราสามารถใช้ PHP ได้สองรูปแบบคือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ PHP เป็นแบบโมดูล PHP จะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงานนั่นเอง ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เพราะว่า ถ้าเป็น CGI แล้ว ตัวแปลชุดคำสั่งของ PHP ถือว่าเป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้นมาทำงานทุกครั้ง ที่ต้องการใช้ PHP ดังนั้น ถ้ามองในเรื่องของประสิทธิภาพในการทำงาน การใช้ PHP แบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

2.5 ลักษณะเด่นของ PHP

1) PHP เป็นโปรแกรมวิ่งข้าง Server ดังนั้นขีดความสามารถไม่จำกัด นั่นคือ PHP วิ่งบนเครื่อง UNIX, Linux, Windows ได้หมด

2) เรียนรู้ง่าย เนื่องจาก PHP ฝังเข้าไปใน HTML และใช้โครงสร้าง และไวยากรณ์ภาษาง่าย ๆ เร็ว และมีประสิทธิภาพ

3) ใช้กับระบบแฟ้มข้อมูลได้

4) ใช้กับข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ

5) ใช้กับโครงสร้างข้อมูลใช้ได้แบบ Scalar, Array, Associative array ใช้กับการประมวลผลภาพได้

2.6 MySQL

MySQL เป็นฐานข้อมูลแบบ open source ที่ได้รับความนิยมในการใช้งานสูงสุดโปรแกรมหนึ่งบนเครื่องให้บริการ มีความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL (Structures Query Language) อย่างมีประสิทธิภาพ มีความรวดเร็วในการทำงาน รองรับการทำงานจากผู้ใช้หลาย ๆ คน และหลาย ๆ งานได้ในขณะเดียวกัน

MySQL ถูกพัฒนาขึ้นโดย MySQL AB โดยมีลิขสิทธิ์การใช้งาน 2 แบบ นั่นคือ ผู้ดูแลระบบสามารถใช้งานซอฟต์แวร์ MySQL ได้โดยไม่มีค่าใช้จ่ายใด ๆ ภายใต้ลิขสิทธิ์ของ GNU General Public License (http://www.gnu.org/licenses/) หรืออาจเลือกใช้แบบที่มีลิขสิทธิ์ทางการค้าของ MySQL AB ซึ่งเป็นผู้ผลิต และพัฒนาซอฟต์แวร์โดยตรงก็ได้ หากไม่ต้องการเกี่ยวข้องกับข้อตกลงเรื่อง GPL รายละเอียดเพิ่มเติมเกี่ยวกับโปรแกรม MySQL สามารถหาข้อมูลได้จาก http://www.MySQL.com

คำอธิบายเพิ่มเติมเกี่ยวกับหน้าที่ ความสามารถและการทำงานของโปรแกรม MySQL มีดังต่อไปนี้

- MySQL ถือเป็นระบบจัดการฐานข้อมูล (DataBase Management System (DBMS))

ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติมเข้าถึงหรือประมวลผลข้อมูลที่เก็บในฐานข้อมูลจำเป็นจะต้องอาศัยระบบจัดการฐานข้อมูล ซึ่งจะทำหน้าที่เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูลทั้งสำหรับการใช้งานเฉพาะ และรองรับการทำงานของแอพลิเคชันอื่น ๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการจัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูล และระบบจัดการฐานข้อมูล

- MySQL เป็นระบบจัดการฐานข้อมูลแบบ relational

ฐานข้อมูลแบบ relational จะทำการเก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์เพียงไฟล์เดียว ทำให้ทำงานได้รวดเร็ว และมีความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหากันทำให้สามารถรวมหรือจัดกลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของโปรแกรม MySQL ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล

- MySQL แจกจ่ายให้ใช้งานแบบ open source

นั่นคือ ผู้ใช้งาน MySQL ทุกคนสามารถใช้งาน และปรับแต่งการทำงานได้ตามต้องการ สามารถดาวน์โหลดโปรแกรม MySQL ได้จากอินเทอร์เน็ต และนำมาใช้งานโดยไม่มีค่าใช้จ่ายใด ๆ

2.7 ความเสี่ยงและวิธีการสร้างความปลอดภัยให้ฐานข้อมูล

ก่อนที่จะกล่าวถึงขั้นตอนการปรับแต่งค่าความปลอดภัยให้กับโปรแกรม MySQL ผู้ดูแลระบบควรจะต้องทราบถึงความเสี่ยงที่เกิดขึ้นจากการใช้งานฐานข้อมูล และหลักปฏิบัติโดยทั่วไปในการสร้างความปลอดภัยให้ฐานข้อมูลก่อน ซึ่งรายละเอียดที่จะอธิบายในหัวข้อนี้จะกล่าวถึงภาพรวม เพื่อให้ผู้ดูแลระบบสามารถนำไปประยุกต์ใช้ได้กับฐานข้อมูลชนิดอื่น ๆ

ความปลอดภัยของฐานข้อมูลเป็นสิ่งสำคัญมาก เนื่องจากข้อมูลที่เก็บไว้ในฐานข้อมูลถือเป็นองค์ประกอบหลักในการดำเนินงานขององค์กร และมีความอ่อนไหวค่อนข้างสูง เช่น ข้อมูลทางธุรกิจ ข้อมูลลูกค้า ข้อมูลพนักงาน ข้อมูลลับ หรือข้อมูลที่เผยแพร่บนเว็บไซต์ขององค์กร วิธีการสร้างความปลอดภัยให้กับฐานข้อมูลค่อนข้างเป็นเรื่องเฉพาะ และมีความซับซ้อนแตกต่างจากการสร้างความปลอดภัยให้กับเครือข่ายหรือระบบปฏิบัติการ

ทั้งนี้ จุดบกพร่องที่ทำให้เกิดความเสี่ยงต่อความไม่ปลอดภัยของฐานข้อมูลมีสาเหตุจากความซับซ้อนของระบบฐานข้อมูล การเก็บรหัสผ่านอย่างไม่ปลอดภัย การตั้งค่าการทำงานที่ผิดพลาด หรือ backdoor ของระบบที่ผู้ดูแลระบบไม่ทราบ การลดความเสี่ยงของข้อบกพร่องเหล่านี้ทำได้โดยการกำหนดหลักปฏิบัติในการใช้งานฐานข้อมูลดังนี้

1) ให้สิทธิ์การใช้งานกับผู้ใช้ตามความจำเป็นเท่านั้น ผู้ใช้งานฐานข้อมูลแต่ละคนควรจะได้รับสิทธิ์การใช้งานเฉพาะที่จำเป็นต่อการดำเนินงานของแต่ละคน

2) ทำการป้องกันในหลายๆ ระดับ เช่น ระดับของการขอเข้าใช้งาน ระดับของสิทธิ์การใช้งาน หรือระดับของขอบเขตของฐานข้อมูลที่ให้ใช้งาน

3) การป้องกันการบุกรุกเป็นสิ่งที่ควรปฏิบัติ แต่ผู้ดูแลจะต้องตรวจสอบการละเมิดความปลอดภัยด้วย

4) นำกระบวนการเข้ารหัสมาใช้งานหากเป็นไปได้

5) กำหนดนโยบายและขั้นตอนปฏิบัติด้านความปลอดภัยที่ชัดเจน รัดกุม

การสร้างความปลอดภัยให้กับฐานข้อมูลจะต้องตั้งอยู่บนพื้นฐานต่อไปนี้ คือ

1) ความลับ และความปลอดภัย : ข้อมูลจะต้องไปถูกเปิดเผยต่อผู้ที่ไม่ได้รับสิทธิ์ในการเข้าถึง

2) ความถูกต้อง ความสมบูรณ์และการตรวจสอบตัวตนผู้ใช้งาน : ข้อมูลจะต้องไม่ถูกแก้ไข หรือยักยอกทั้งโดยเจตนาร้าย หรือโดยไม่เจตนาก็ตาม นอกจากนั้น จะต้องพิสูจน์ได้ว่าต้นทางของข้อมูลมาจากที่ใดหรือใคร

3) ความพร้อมใช้ และความสามารถในการกู้คืน : ระบบฐานข้อมูลจะต้องถูกปกป้องให้พร้อมใช้งานได้ตลอดเวลา รวมถึงจะต้องกู้คืนได้หากข้อมูลสูญหาย

นอกจากนั้น การสร้างความปลอดภัยให้กับฐานข้อมูลจำเป็นต้องมั่นใจว่าได้มีการป้องกันถึงระดับลึก ได้แก่ การสร้างความปลอดภัยให้กับเครือข่าย ซึ่งอาจทำได้โดยการป้องกันที่ไฟร์วอลล์ เราเตอร์ ระบบตรวจจับผู้บุกรุก (IDS) และการสร้างความปลอดภัยให้กับระบบปฏิบัติการ เพื่อให้

แน่ใจได้ว่าการเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาตจะไม่เป็นผลมาจากการกำหนดค่าที่ผิดพลาดให้กับระบบปฏิบัติการ และอุปกรณ์เหล่านั้น

หลักการสำคัญในการสร้างความปลอดภัยให้กับฐานข้อมูลนั้น ผู้ดูแลระบบควรจะคำนึงถึงองค์ประกอบต่อไปนี้ เพื่อนำไปพิจารณาประยุกต์ใช้กับระบบฐานข้อมูลของตนเองตามความเหมาะสม

1) การตรวจสอบตัวตนผู้ใช้งาน

จะต้องมั่นใจว่ามีการตรวจสอบตัวตนของผู้ใช้งานทุกคนที่ติดต่อกับฐานข้อมูล ในระดับต่ำสุดคือการนำเอารหัสผ่านมาใช้งานสำหรับทุกการติดต่อ ซึ่งรหัสผ่านเหล่านี้จะต้องได้รับการเก็บรักษาอย่างปลอดภัยในฐานข้อมูลและถูกเข้ารหัสอย่างเหมาะสม ควรมีข้อกำหนดเรื่องการใช้งานรหัสผ่าน ได้แก่ กำหนดความยาวขั้นต่ำของรหัสผ่านที่ใช้ กำหนดว่ารหัสผ่านจะต้องประกอบด้วยตัวอักษรหรือตัวเลขรวมกับอักขระพิเศษ และไม่ให้ใช้งานรหัสผ่านที่เดาได้ง่าย เป็นต้น

2) การควบคุมการเข้าถึงออบเจ็กต์ใด ๆ และการตรวจสอบแอพลิเคชันที่อนุญาตให้ใช้งาน

ออบเจ็กต์ของฐานข้อมูลประกอบด้วย ตาราง ซินโนนีมม์ (synonymn) วิว (view) อินเด็กซ์ (index) สตอร์โพรซีเจอร์ (store procedure) และทริกเกอร์ (trigger) ซึ่งสามารถควบคุมการอนุญาตให้เข้าถึงออบเจ็กต์เหล่านี้ได้โดยกำหนดไว้ที่สิทธิ์การใช้งานฐานข้อมูล ซึ่งควรได้รับการกำหนดตั้งแต่ขั้นตอนของการออกแบบ ทั้งนี้ผู้ดูแลฐานข้อมูลหรือผู้ออกแบบฐานข้อมูลจะต้องคำนึงถึงหลักการที่จะให้สิทธิ์แก่ผู้ใช้งานแต่ละคนให้น้อยที่สุดเท่าที่จะเป็นไปได้ การควบคุมการเข้าถึงออบเจ็กต์เหล่านี้ มีวิธีการที่แตกต่างกันตามแต่ละชนิดของออบเจ็กต์ เช่น การใช้ซินโนนีมม์จะช่วยให้การอ้างถึงแต่ละตารางในฐานข้อมูลสามารถทำได้โดยไม่จำเป็นต้องทราบว่าเจ้าของตารางดังกล่าวคือใคร เป็นการซ่อนโครงสร้างของฐานข้อมูลจากผู้ใช้งานโดยที่ผู้ดูแลยังสามารถตรวจสอบได้ว่าใครมาใช้ตารางใดในฐานข้อมูลบ้าง การสร้างความปลอดภัยให้กับออบเจ็กต์วิว ทำได้โดยการควบคุมการเข้าถึงในระดับแถวและคอลัมน์ก่อนที่แต่ละตารางจะถูกนำมารวมไว้ด้วยกัน เป็นต้น หรือหากใช้งานสถาปัตยกรรม 3-tier ซึ่งมีแอพลิเคชันเซิร์ฟเวอร์ทำหน้าที่รอรับการเรียกใช้งานแอพลิเคชันทั้งหมดจากเครื่องขอเข้าใช้บริการและติดต่อกับฐานข้อมูล จำเป็นต้องกำหนดให้เครื่องขอใช้งานแสดงตัวตนกับเครื่องแอพลิเคชันเซิร์ฟเวอร์ และให้แอพลิเคชันเซิร์ฟเวอร์แสดงตัวตนกันกับฐานข้อมูลก่อนจึงจะอนุญาตให้เข้าใช้งานตามต้องการได้

3) นโยบายและขั้นตอนปฏิบัติในการดูแลระบบ

ต้องกำหนดนโยบายที่ชัดเจนเกี่ยวกับการใช้งาน และการดูแลระบบ พร้อมทั้งกำหนดขั้นตอนปฏิบัติต่างๆ มาบังคับใช้ตามนโยบายดังกล่าวเป็นลายลักษณ์อักษร โดยแสดงรายละเอียดถึงข้อบังคับด้านความปลอดภัยและการบริหารความเสี่ยง ภายในต้องประกอบด้วยมาตรฐานการใช้งานบัญชีรายชื่อผู้ใช้ รหัสผ่าน กฎ และออบเจ็กต์ รวมถึงการตรวจสอบและการบันทึกล็อก

4) การใช้งนค่า configuration เริ่มต้นที่ปลอดภัย

ฐานข้อมูลบางชนิดจะมีชื่อผู้ใช้ และรหัสผ่านที่กำหนดไว้เป็นค่าดีฟอลต์เริ่มต้น ซึ่งเป็นที่ทราบกันดีในกลุ่มผู้ใช้ ค่าดังกล่าวนี้ทำให้ผู้ที่ทราบสามารถเข้าถึงฐานข้อมูลได้ในหลายระดับ ดังนั้นผู้ดูแลจึงควรยกเลิกหรือเปลี่ยนแปลงค่ารหัสผ่านทันทีหลังจากเข้าใช้งานครั้งแรก นอกจากนั้น ไฟล์ที่เกี่ยวข้องกับการทำงานของระบบฐานข้อมูลจะต้องได้รับการจำกัดการเข้าถึง ทั้งเพื่ออ่าน เขียนหรือเรียกใช้งานจากผู้ไม่เกี่ยวข้อง เพื่อที่ผู้บุกรุกจะไม่สามารถเปลี่ยนแปลงค่าการทำงานใด ๆ ได้ สิ่งที่สำคัญที่สุดก็คือ ผู้ดูแลระบบจะต้องปรับแต่งค่าการทำงานให้เหมาะสมกับระบบและการใช้งานของตน

5) การตรวจสอบการทำงาน

การตรวจสอบการทำงานของฐานข้อมูลช่วยให้ผู้ดูแลสามารถตรวจจับกิจกรรมที่เกิดขึ้นโดยไม่ได้รับอนุญาตหรือกิจกรรมที่มีจุดประสงค์ร้าย กิจกรรมที่ควรได้รับการตรวจสอบระบบประกอบด้วย

- ความพยามยามในการติดต่อฐานข้อมูลที่ไม่ประสบความสำเร็จ
- การเปิดและปิดฐานข้อมูล
- การเรียกดู การแก้ไขและการลบข้อมูลออกจากตาราง
- การสร้างและการลบออบเจ็กต์
- การเรียกใช้งานโปรแกรม

ผู้ดูแลควรจัดเก็บข้อมูลเหล่านี้ไว้ในรูปของไฟล์ล็อกหรือฐานข้อมูลล็อก ซึ่งข้อมูลที่ควรเก็บบันทึกในล็อกประกอบด้วย ใครเป็นผู้สร้างข้อมูล ใครเป็นผู้แก้ไขข้อมูล และข้อมูลใดที่ถูกเปลี่ยนแปลงแก้ไข เป็นต้น

6) แผนการสำรองข้อมูลและการกู้คืนระบบ

ความเสียหายของฐานข้อมูล การถูกทำลายโดยอุบัติเหตุ และกิจกรรมที่เกิดขึ้นโดยไม่ได้รับอนุญาต หรือมีจุดประสงค์ร้ายต่อฐานข้อมูล อาจนำไปสู่ความเสียหายอย่างรุนแรงของฐานข้อมูล หากขาดแผนการสำรองข้อมูลที่เหมาะสม กระบวนการสำรองข้อมูล และการกู้คืนระบบควรจะได้รับการทดสอบในช่วงเวลาปกติ และการเก็บข้อมูลสำรองไว้ภายนอกองค์กรจะช่วยให้การ

กู้คืนข้อมูลจากความเสียหายทำได้รวดเร็ว กระบวนการสำรองข้อมูลควรจะได้รับการทดสอบให้มั่นใจว่า

- พนักงานเกิดความเชื่อมั่นต่อวิธีการกู้คืนข้อมูล
- แผนการสำรองข้อมูลและการกู้คืนระบบได้รับการวิเคราะห์ตรวจสอบอย่างเหมาะสม
- ผู้ดูแลสามารถอ่านข้อมูลจากเทปสำรองข้อมูลโดยใช้ไดรฟ์อื่นต่างหากจากที่ใช้ในการเขียนข้อมูลได้

นอกจากนั้น แผนการสำรองข้อมูลจะต้องกำหนดถึงวิธีการในการสำรองข้อมูล ซึ่งมีทางเลือกให้ใช้งานได้หลายรูปแบบ ได้แก่

- การสำรองข้อมูลแบบ cold คือการสำรองข้อมูลในขณะที่ไม่มีการใช้งานฐานข้อมูล
- การสำรองข้อมูลแบบ hot คือการสำรองข้อมูลในขณะที่ฐานข้อมูลถูกใช้งาน
- การสำรองข้อมูลแบบ logical คือการสำรองข้อมูลในช่วงเวลาใดช่วงเวลาหนึ่งในขณะที่ฐานข้อมูลถูกใช้งาน

7) การสร้างความปลอดภัยให้โปรแกรม MySQL

ผู้ดูแลระบบที่ใช้งานโปรแกรม MySQL เป็นฐานข้อมูลในเครื่องให้บริการใด ๆ จำเป็นต้องทราบถึงวิธีการสร้างความปลอดภัยให้กับโปรแกรม MySQL ที่ใช้งาน เนื่องจากการใช้งานฐานข้อมูลทำให้เกิดความเสี่ยงต่อความปลอดภัยของเครื่องตามที่ได้อธิบายแล้วข้างต้น สำหรับหัวข้อนี้จะแสดงรายละเอียดถึงวิธีการในการสร้างความปลอดภัยให้โปรแกรม MySQL บนระบบปฏิบัติการ Red Hat Linux โดยเฉพาะหากผู้ดูแลระบบติดตั้งโปรแกรม MySQL โดยเลือกติดตั้งในขณะที่ติดตั้งระบบปฏิบัติการ หรือติดตั้งโดยใช้แพ็คเกจชนิด RPM จะมีข้อดีคือ ผู้ดูแลระบบจะสามารถใช้โปรแกรม up2date (ตามที่ได้อธิบายไว้ในบทก่อนหน้านี้) ในการตรวจสอบแก้ไขช่องโหว่ที่เกิดขึ้นกับโปรแกรมได้ ในทางตรงกันข้าม หากผู้ดูแลระบบเลือกติดตั้งโปรแกรมโดยคอมไพล์จากไฟล์ต้นฉบับด้วยตนเอง จะมีข้อดีคือโปรแกรม MySQL ที่ได้จะมีความยืดหยุ่นมากกว่า ผู้ดูแลระบบสามารถเลือกออปชัน และไลบรารี่ที่จะใช้งานได้ตามต้องการมากกว่า อย่างไรก็ตาม ไม่มีออปชันใดๆ เกี่ยวข้องกับการสร้างความปลอดภัยที่ควรได้รับการพิจารณาเป็นพิเศษในการติดตั้งโปรแกรม MySQL โดยการคอมไพล์จากไฟล์ต้นฉบับ จึงไม่นำมาอธิบายในที่นี้ สำหรับผู้ดูแลระบบที่ต้องการดาวน์โหลดโปรแกรม MySQL หรือตรวจสอบเวอร์ชันของโปรแกรม MySQL ที่จะใช้งาน สามารถหาข้อมูลได้ที่ http://www.MySQL.com/downloads/index.html

โปรแกรม MySQL ทำงานเป็นฐานข้อมูล และระบบจัดการฐานข้อมูลบนเครื่องให้บริการ โดยเปิดให้ผู้ใช้งานติดต่อฐานข้อมูลผ่านพอร์ต 3306 บนโพรโตคอล TCP ของเครื่องให้บริการ (ค่าดีฟอลต์ของโปรแกรม) หลังจากที่สั่งให้โปรแกรม MySQL เริ่มต้นทำงานจะเกิดการสร้างเดมอนชื่อ MySQL ไว้รอรับการติดต่อ ซึ่งการใช้งานฐานข้อมูลทำได้ 2 วิธีคือ การเข้าใช้ฐานข้อมูลโดยตรงผ่านโปรแกรม MySQL และการใช้งานผ่านโปรแกรมที่เขียนขึ้นเพื่อใช้ติดต่อฐานข้อมูล เช่น โปรแกรมที่ถูกเขียนขึ้นด้วยภาษา PHP เป็นต้น ผู้ที่จะเข้าใช้งานฐานข้อมูลได้จะต้องได้รับการตรวจสอบสิทธิ์ และพิสูจน์ตัวตนผู้ใช้ ซึ่งบัญชีรายชื่อผู้ใช้ของโปรแกรม MySQL นี้แยกจากบัญชีผู้ใช้งานของระบบโดยเด็ดขาด ไม่มีความเกี่ยวข้องกันแต่อย่างใด โดยจะถูกจัดเก็บและจัดการผ่านฐานข้อมูลของ MySQL ที่ใช้งาน นอกจากนั้น ผู้ดูแลระบบควรจะสร้างผู้ใช้งานในระบบชื่อ MySQL และกลุ่มผู้ใช้ชื่อ MySQL มารองรับการทำงานของโปรแกรม MySQL ซึ่งจะอธิบายถึงการนำไปใช้ในลำดับต่อไป

วิธีการสร้างความปลอดภัยให้กับโปรแกรม MySQL ทำได้ในหลายระดับ ซึ่งผู้ดูแลระบบสามารถเลือกนำไปปฏิบัติได้ตามรูปแบบและจุดประสงค์การใช้งาน แบ่งเป็นส่วนๆ ได้ดังนี้

- การเริ่มต้นใช้งาน และการเรียกใช้งานโปรแกรม MySQL
- ระบบและวิธีการตรวจสอบสิทธิ์ของโปรแกรม MySQL
- ไฟล์ล็อกของโปรแกรม MySQL
- การจัดการเกี่ยวกับเจ้าของไฟล์ที่เกี่ยวข้องกับโปรแกรม MySQL ในระบบปฏิบัติการ
- ข้อควรระวังที่เกี่ยวข้องกับความปลอดภัยของโปรแกรม MySQL