นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน)

ฉบับแก้ไขครั้งที่ 6

วันที่ 13 พฤศจิกายน 2567

อนุมัติเมื่อ 13 พ.ย. 2567 (BOD 4/2567)

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.วัตถุประสงค์

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นการกำหนดกฎระเบียบเพื่อป้องกันการเกิดอุบัติเหตุในการใช้ทรัพย์สินด้านสารสนเทศ (Information Asset) ของบริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน) และ บริษัทย่อย ("บริษัทฯ") อาทิ การเปลี่ยนแปลงข้อมูล การเสียหายของข้อมูล การรั่วไหลของข้อมูล ไม่ว่าจะเกิดขึ้นจากความตั้งใจหรือไม่ก็ตาม ผู้ที่ใช้ทรัพย์สินทางด้านสารสนเทศของบริษัทฯ ต้องตระหนักถึงความสำคัญด้านการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. ขอบเขตที่ครอบคลุม

2.1) คำจำกัดความของทรัพย์สินด้านสารสนเทศ

ทรัพย์สินด้านสารสนเทศ หมายถึง ระบบสารสนเทศหรือข้อมูลที่ใช้ในระบบสารสนเทศ

ระบบสารสนเทศ (Information System) หมายถึง ระบบที่มีการนำคอมพิวเตอร์มาช่วยในการรวบรวม จัดเก็บ หรือจัดการกับข้อมูล เพื่อให้ข้อมูลนั้นกลายเป็นสารสนเทศที่ดี สามารถนำไปใช้ในการประมวลผลเพื่อใช้ประกอบการตัดสินใจในการดำเนินงานได้อย่างรวดเร็วและมีประสิทธิภาพ ดังนั้น ระบบสารสนเทศ จึงประกอบด้วยองค์ประกอบสำคัญ คือ Hardware, Software, ผู้ใช้งาน (User), ข้อมูล (Data), และ ขั้นตอนการทำงานในระบบสารสนเทศ (Procedure)

คอมพิวเตอร์ (Computer) หมายถึง อุปกรณ์คอมพิวเตอร์, เซิร์ฟเวอร์, คอมพิวเตอร์ส่วนบุคคล, อุปกรณ์เกี่ยวกับข้อมูลแบบพกพา (เช่น แท็บเล็ต หรือโทรศัพท์มือถือ), อุปกรณ์ต่อพ่วง, อุปกรณ์หน่วยความจำ (เช่น จานแม่เหล็ก หรือที่เรียกว่า Magnetic Disk) ที่ประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์

ฮาร์ดแวร์ (Hardware) หมายถึง ส่วนกายภาพของเครื่องคอมพิวเตอร์ แบ่งเป็น 3 ส่วนใหญ่ คือ 1) หน่วยรับข้อมูล ได้แก่ แป้นพิมพ์ หน่วยบันทึกข้อมูล 2) หน่วยความจำ ได้แก่ ส่วนของการบันทึกข้อมูล 3) หน่วยแสดงผล ได้แก่ จอภาพ เครื่องพิมพ์ เป็นต้น ทั้งนี้ยังรวมถึงอุปกรณ์ทางกายภาพประกอบอื่นๆ ที่เกี่ยวข้อง

ซอฟต์แวร์ (Software) หมายถึง โปรแกรมคอมพิวเตอร์ หรือส่วนชุดคำสั่งที่เขียนขึ้นมาด้วยภาษาคอมพิวเตอร์ ภาษาใดภาษาหนึ่ง ที่เครื่องคอมพิวเตอร์สามารถแปลภาษา รับรู้ได้ และสั่งการให้คอมพิวเตอร์ทำงานในลักษณะที่ต้องการภายใต้ขอบเขตความสามารถที่เครื่องคอมพิวเตอร์หรือโปรแกรมนั้นสามารถทำได้

ข้อมูล (Data) หมายถึง ข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายหรือระบบสารสนเทศ

ระบบเครือข่าย (Network) หมายถึง ระบบที่มีการนำคอมพิวเตอร์อย่างน้อย 2 เครื่องมาเชื่อมต่อกัน โดยใช้สื่อกลางในการสื่อสารข้อมูลถึงกันได้อย่างมีประสิทธิภาพ ซึ่งทำให้ผู้ใช้คอมพิวเตอร์แต่ละเครื่องสามารถแลกเปลี่ยนข้อมูลซึ่งกันและกันได้ ได้แก่ ระบบแลน (LAN: Local Area Network), ระบบเครือข่ายแบบไร้สาย (Wi-Fi หรือ Wireless Fidelity) หรือ WLAN: Wireless LAN

2.2) **ผู้ที่อยู่ภายใต้นโยบายฯ**

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้ มีขอบเขตการบังคับใช้ ครอบคลุมถึงกรรมการ ผู้บริหาร และพนักงานทุกคนของบริษัทฯ รวมถึงผู้เกี่ยวข้องกับทรัพย์สินด้านสารสนเทศที่ได้รับการอนุญาตให้ใช้งานได้ภายใต้การควบคุมดูแลที่เหมาะสม โดยผู้ควบคุมตามที่เห็นสมควร

2.3) **อุปกรณ์ที่อยู่ภายใต้นโยบายฯ**

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้ มีขอบเขตครอบคลุมอุปกรณ์ระบบสารสนเทศและข้อมูลสารสนเทศทั้งหมดที่เป็นกรรมสิทธิ์ของบริษัทฯ อันได้แก่ คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย อุปกรณ์จากหน่วยงานภายนอก คอมพิวเตอร์ส่วนบุคคลของพนักงาน คอมพิวเตอร์ของผู้รับเหมาที่นำมาใช้ในการปฏิบัติงานของบริษัทฯ ซึ่งได้รับการอนุญาตให้ใช้งานได้ภายใต้การควบคุมดูแลที่เหมาะสม โดยผู้ควบคุมตามที่เห็นสมควร

3. การควบคุมดูแลคอมพิวเตอร์

3.1) **การนำอุปกรณ์คอมพิวเตอร์ และสื่อบันทึกข้อมูล เข้ามาใช้งาน**

1) ห้ามมิให้นำคอมพิวเตอร์ อุปกรณ์ที่เกี่ยวข้องกับซอฟต์แวร์ เข้ามาใช้โดยพลการ โดยไม่ได้รับการอนุญาตจากฝ่ายไอซีที
2) ต้องเลือกชนิดของอุปกรณ์ที่มีระบบการป้องกันและรักษาความปลอดภัยอยู่เสมอ เช่น มีซอฟต์แวร์สำหรับป้องกันไวรัสที่บริษัทฯ ใช้งานอยู่
3) กรณีการติดตั้ง Server และคอมพิวเตอร์นั้น ต้องเลือกผู้จำหน่าย/ผู้รับเหมา(Supplier) ที่สามารถให้บริการแบบ Onsite Service ได้ เพื่อป้องกันการรั่วไหลของข้อมูลของบริษัทฯ และเป็นการดูแลรักษาข้อมูลที่เป็นความลับของบริษัทฯ ตามนโยบายฯ
4) กรณีการควบคุมดูแล Software ที่จะนำมาใช้กับ Server และคอมพิวเตอร์นั้น ฝ่ายไอซีทีต้องควบคุมจำนวน License และจำนวนเครื่องคอมพิวเตอร์ที่ Install เพื่อใช้งานจริง และต้องจัดเก็บเอกสารการรับประกันและสื่อบันทึกข้อมูล (Media) ไว้อย่างเหมาะสม
5) เครื่องคอมพิวเตอร์ของบริษัท ไม่อนุญาตให้สามารถใช้งานสื่อบันทึกข้อมูลภายนอก เช่น Flash drive, hard disk external ได้
6) อุปกรณ์บันทึกอื่นของบริษัท ที่มีการใช้งานประจำ เช่น อุปกรณ์บันทึกภาพมุมสูง (โดรน), กล้องถ่ายภาพ จะต้องแจ้งขอต่อฝ่ายไอซีที เพื่อให้ดำเนินการลงทะเบียน (ล็อคซีเรียลประจำเครื่อง) เพื่อให้สามารถดึงข้อมูลเข้าคอมพิวเตอร์ได้

7) กรณีต้องการใช้งานสื่อบันทึกข้อมูลภายนอกตามข้อ 5) ต้องมีการเปิดใบงานผ่านระบบงานของฝ่ายไอซีที เพื่อดำเนินการปลดล็อคชั่วคราวให้สามารถใช้งานได้

3.2) **การซ่อมแซมอุปกรณ์คอมพิวเตอร์ และสื่อบันทึกข้อมูล**

1) เมื่อคอมพิวเตอร์ชำรุด ฝ่ายไอซีที จะต้องดูแลการซ่อมแซมอุปกรณ์คอมพิวเตอร์ ภายใต้ความเห็นชอบของฝ่ายไอซีที

2) ห้ามมิให้นำอุปกรณ์คอมพิวเตอร์ไปซ่อมแซมนอกบริษัทฯ ฝ่ายไอซีที จะต้องติดต่อผู้จำหน่าย/ผู้รับเหมา (Supplier) เข้ามาดำเนินการซ่อมแซมที่บริษัทฯ สำหรับกรณีที่จำเป็นต้องนำอุปกรณ์ฯ ออกไปซ่อมนอกบริษัทฯ ห้ามมิให้นำอุปกรณ์สำหรับเก็บบันทึกข้อมูล เช่น Hard Disk ออกไปด้วย จะต้องถอดออกและจัดเก็บไว้ที่บริษัทฯ

3) กรณีที่จำเป็นต้องซ่อมแซมอุปกรณ์สำหรับเก็บบันทึกข้อมูล เช่น Hard Disk ภายนอกบริษัทฯ ต้องเลือกผู้จำหน่าย/ผู้รับเหมา (Supplier) ที่น่าเชื่อถือ

3.3) **การทิ้งอุปกรณ์คอมพิวเตอร์ และสื่อบันทึกข้อมูล**

1) การทิ้งอุปกรณ์คอมพิวเตอร์นั้นต้องได้รับความเห็นชอบจากฝ่ายไอซีทีก่อน และฝ่ายไอซีทีจะต้องดำเนินการปฏิบัติตามขั้นตอนการขายทรัพย์สินเสื่อมสภาพ ตามเอกสาร ระเบียบปฏิบัติการบันทึกและการตรวจทรัพย์สินของแผนกทะเบียนทรัพย์สิน

2) ฝ่ายไอซีที จะเป็นผู้ดำเนินการทำลายสื่อบันทึกข้อมูล เช่น Hard Disk โดยจะต้องดำเนินการลบข้อมูลในสื่อบันทึกข้อมูลทั้งหมด หรือทำลายอุปกรณ์สื่อบันทึกข้อมูลดังกล่าวทางกายภาพให้เรียบร้อยก่อนที่จะนำไปทำลายและทิ้ง โดยมีขั้นตอนการลบข้อมูลสำหรับสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทของสื่อบันทึกข้อมูล	ขั้นตอนการลบข้อมูลในสื่อบันทึกข้อมูล	ขั้นตอนการทำลายสื่อบันทึกข้อมูล
1) Optical Media เช่น CD, DVD, BD	ไม่มี	ทำลายทางกายภาพ จนไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้อีก เช่น ตัดเป็นชิ้นเล็กๆ การเจาะ การทุบทำลาย หรือเผาจนไหม้ เป็นต้น
2) สื่อแม่เหล็ก เช่น Tape Backup	ไม่มี	
3) สื่อแม่เหล็ก เช่น SATA Hard Disk, SCSI Hard Disk	เขียนทับข้อมูลเดิมอย่างน้อย 1 ครั้ง (Format>เขียนทับ>Format)	
4) Flash Memory Storage เช่น SSD, Flash Drive, Memory Card, NVME	เขียนทับข้อมูลเดิมอย่างน้อย 1 ครั้ง (Format>เขียนทับ>Format)	

4. ข้อปฏิบัติเกี่ยวกับการใช้คอมพิวเตอร์

4.1) ข้อปฏิบัติทั่วไป

1) คอมพิวเตอร์ จะต้องใช้เพื่อการดำเนินงานของบริษัทฯ เท่านั้น นอกจากนี้ ผู้ที่ได้รับคอมพิวเตอร์ จะต้องพยายามใช้คอมพิวเตอร์ เพื่อส่งเสริมการดำเนินธุรกิจของบริษัทฯ ห้ามมิให้ใช้คอมพิวเตอร์เพื่อกิจส่วนตัวหรือกิจการอื่น นอกเหนือจากการดำเนินธุรกิจของบริษัทฯ
2) ฝ่ายไอซีที จะต้องกำหนดสิทธิในการเข้าถึงข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์อย่างเหมาะสม เพื่อป้องกันการรั่วไหลหรือการสูญหายของข้อมูล นอกจากนี้ ผู้ใช้คอมพิวเตอร์จะต้องพยายามป้องกันไม่ให้เกิดการรั่วไหลหรือเกิดการสูญหายของข้อมูลเท่าที่จะสามารถทำได้ตามสิทธิของตน ห้ามมิให้เข้าถึงข้อมูลที่อยู่นอกเหนือสิทธิของตน
3) ห้ามติดตั้งโปรแกรมที่ไม่จำเป็นในการปฏิบัติงานลงในเครื่องคอมพิวเตอร์ และห้ามติดตั้งโปรแกรมที่ไม่มี License โดยเด็ดขาด แม้ว่าโปรแกรมที่ติดตั้งนั้น จะมีความจำเป็นในการปฏิบัติงานก็ตาม
4) ห้ามติดตั้งซอฟต์แวร์ที่บริษัทฯ หรือฝ่ายไอซีที ประกาศสั่งห้ามใช้งาน ลงในเครื่องคอมพิวเตอร์
5) ห้ามมิให้บุคคลอื่น เปลี่ยนแปลงการตั้งค่าคอมพิวเตอร์ที่ฝ่ายไอซีทีได้ทำการตั้งค่าไว้โดยพลการ
6) การจัดเก็บข้อมูล และการดูแลรักษาข้อมูลในคอมพิวเตอร์นั้น จะต้องพิจารณาความจำเป็นในการสำรองข้อมูล (Back up data) ตามระดับความสำคัญของข้อมูล และควรสำรองข้อมูลเป็นประจำสม่ำเสมอ โดยต้องมีการสำรองข้อมูลสำคัญไว้ใน File Sharing Server ทั้งนี้ ต้องกำหนดจำนวนของการสำรองข้อมูลในสื่อบันทึกข้อมูล (Back up Media) ของ Server และสถานที่จัดเก็บรักษาข้อมูลให้ปลอดภัย
7) โทรศัพท์มือถือและ Smart Phone ที่นำมาใช้งาน จะต้องใช้ระบบการรักษาความปลอดภัยของข้อมูล (Security Lock) เช่น Dial Lock, Key Lock และควรนำซอฟต์แวร์สำหรับป้องกันไวรัสมาใช้งานด้วย

4.2) มาตรการด้านความปลอดภัย

1) ฝ่ายไอซีที จะสั่งการไปยังผู้ที่อยู่ภายใต้นโยบายฯ เกี่ยวกับมาตรการด้านความปลอดภัยที่เหมาะสม และตรวจสอบว่าผู้ที่อยู่ภายใต้นโยบายฯ ได้ดำเนินการตามมาตรการด้านความปลอดภัยสม่ำเสมอ
2) เครื่องคอมพิวเตอร์ จะต้องมีการตั้งค่า Force Lock Screen อัตโนมัติ หากไม่ได้ใช้งานเป็นระยะเวลา 15 นาที (Time Idle)
3) ระบบ ERP จะต้องมีการตั้งค่า Force Log Out อัตโนมัติ หากไม่ได้ใช้งานเป็นระยะเวลา 15 นาที

4) รหัสผ่าน (Password) ในการเข้าใช้งานคอมพิวเตอร์ และระบบ ERP จะต้องกำหนดให้รหัสผ่านเดิม (Password History) มีอายุ 365 วัน จึงจะสามารถนำรหัสผ่านเดิมนั้น กลับมาใช้งานได้อีก

5) สำหรับเครื่องคอมพิวเตอร์และ Server จะต้องมีการนำซอฟต์แวร์สำหรับป้องกันไวรัสมาใช้งาน และจะต้องรักษา Version, Scan Engine, Pattern File ให้อยู่ในสภาพใหม่ล่าสุดอยู่เสมอ นอกจากนี้ จะต้องตั้งค่าเปิดการใช้งานของซอฟต์แวร์สำหรับป้องกันไวรัสให้มีการทำงานอยู่เสมอ และต้องตั้งค่าให้มีการตรวจสอบอีเมล การดาวน์โหลดไฟล์ (Download File) และการคัดลอกไฟล์ (Copy File) ด้วย

6) กรณีที่คาดว่าจะมีการติดไวรัส ให้ผู้ที่อยู่ภายใต้นโยบายฯ ถอดสายเคเบิ้ลที่เชื่อมต่อกับระบบเครือข่ายออก และรายงานต่อฝ่ายไอซีที ทั้งนี้ต้องให้ความร่วมมือในการหาสาเหตุและกำจัดไวรัส

7) มาตรการด้านความปลอดภัยของ Operating System และ Application เช่น สำหรับคอมพิวเตอร์ของสำนักงาน จะต้อง Update Windows ของ MS-Windows เป็นประจำทุกสัปดาห์

8) คอมพิวเตอร์ที่ใช้ Operating System ซึ่ง Security Support ของบริษัทผู้ผลิตได้สิ้นสุดลงแล้ว ห้ามมิให้เชื่อมต่อเข้ากับระบบเครือข่ายของบริษัทฯ

9) เพื่อป้องกันข้อมูลสูญหาย ควรมีการเข้ารหัส Hard Disk ของคอมพิวเตอร์

4.3) มาตรการเกี่ยวกับรหัสผ่าน (Password) เพื่อการใช้งาน

1) ผู้ใช้งานที่ได้ขอเพิ่ม แก้ไข หรือยกเลิกสิทธิการใช้งาน และได้รับการอนุมัติจากระดับผู้จัดการขึ้นไป ผ่านในระบบ IT Care จะต้องดำเนินการดูแลรักษารหัสผ่าน (Password) ที่ได้รับมาอย่างระมัดระวังและรอบคอบ โดยต้องปฏิบัติตามข้อควรระวัง ดังนี้

- ห้ามไม่ให้ผู้อื่นยืมรหัสผ่าน (Password) ไปใช้งาน หรือห้ามใช้งานร่วมกัน
- ต้องไม่กำหนดรหัสผ่านที่ผู้อื่นสามารถคาดเดาได้ง่าย กล่าวคือ รหัสผ่านต้องมีความยาว**ตั้งแต่ 8 ตัวอักษรขึ้นไป** และมีการผสมตัวอักษร ได้แก่ ตัวเลข (0-9), ตัวพิมพ์ใหญ่ (A-Z), ตัวพิมพ์เล็ก (a-z), ตัวอักษรพิเศษ (เช่น # & ! @ $ % ^ เป็นต้น)
- ไม่จดบันทึกรหัสผ่าน (Password) ไว้ในที่ที่ผู้อื่นสามารถเห็นได้ง่าย เช่น หน้าจอคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น หากจำเป็นต้องจดบันทึก ให้จัดเก็บไว้ในที่มิดชิดปลอดภัย เช่น จดบันทึกลงสมุด และเก็บไว้ในลิ้นชักที่มีกุญแจล็อคได้ เป็นต้น
- ต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วัน
- ต้องระมัดระวัง ไม่ใส่รหัสผ่าน (Password) ให้ผู้อื่นเห็น
- ใส่รหัสผ่านผิด 5 ครั้งรหัสผ่านจะถูกล็อค (ต้องเปิดใบงานในระบบ IT Care เพื่อขอให้แก้ไข)

2) รหัสผ่าน (Password) สิทธิสูงสุดของระบบ Operating System ทั้งของระบบ Windows Unix / Linux กำหนดให้มีหมดอายุ 90 วัน โดยต้องกำหนดรหัสผ่าน ให้ยากกว่ารหัสผ่านของผู้ใช้งานทั่วไป กล่าวคือ รหัสผ่านต้องมีความยาว**ตั้งแต่ 12 ตัวอักษรขึ้นไป** และมีการผสมตัวอักษร ได้แก่ ตัวเลข (0-9), ตัวพิมพ์ใหญ่ (A-Z), ตัวพิมพ์เล็ก (a-z), ตัวอักษรพิเศษ (เช่น # & ! @ $ % ^ เป็นต้น) กำหนดให้ผู้จัดการฝ่ายไอซีที เป็นผู้ดำเนินการ

3) รหัสผ่าน (Password) ของโปรแกรมการทำงานในระบบ ERP ที่เป็นรหัสผ่านของ Script Program ซึ่งไม่ใช่รหัสผ่านที่ใช้ในการทำงานปกติ เป็นต้น ถือเป็นรหัสผ่านของ Script การทำงานที่ฝังอยู่ในโปรแกรมโดยผู้พัฒนาโปรแกรม จะสงวนสิทธิ์งดเว้นการเปลี่ยนรหัสผ่านหากไม่จำเป็น เพื่อเป็นการป้องกัน Script การทำงานของโปรแกรมไม่ให้การทำงานเกิดความผิดพลาด (รายละเอียดตามภาคผนวก ก.รายละเอียดยูสเซอร์เนมระบบงาน ERP)

4) รหัสผ่าน (Password) ของผู้ให้บริการดูแลระบบ ที่ใช้สำหรับการเชื่อมต่อ VPN ที่ได้รับการร้องขอจากอีเมล และได้รับการอนุมัติเรียบร้อยแล้ว จะมีอายุการใช้งาน 48 ชั่วโมงต่อการร้องขอ 1 ครั้ง และใช้กฎการกำหนดรหัสผ่านเช่นเดียวกับรหัสผ่านของผู้ใช้งานทั่วไป

5) กำหนดให้มีการทบทวน ตรวจทานสิทธิ์การใช้งานระบบเป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง

4.4) การนำคอมพิวเตอร์แบบ Notebook ออกไปใช้งานภายนอกบริษัทฯ

1) ผู้ใช้งาน (User) ต้องระมัดระวังมิให้เกิดการสูญหาย ถูกขโมย หรือเกิดการชำรุดเสียหาย กรณีที่เกิดการสูญหาย ถูกขโมย หรือเกิดการชำรุดเสียหาย ต้องรายงานต่อฝ่ายไอซีทีทันที

2) การนำคอมพิวเตอร์แบบ Notebook ออกไปใช้งานภายนอกบริษัทฯ มีความเสี่ยงของการรั่วไหลของข้อมูลและมีความเสี่ยงต่อไวรัสคอมพิวเตอร์มากขึ้น ผู้ใช้งาน (User) จึงต้องตระหนักถึงความปลอดภัยให้มากยิ่งขึ้น เช่น ต้องมีการเปลี่ยนรหัสผ่าน มีมาตรการป้องกันไวรัส ไม่จดบันทึกรหัสผ่านไว้ในส่วนใดของเครื่องคอมพิวเตอร์ และเพิ่มความถี่ในการอัพเดท Windows

5. ระบบเครือข่าย

5.1) ข้อมูลทั่วไป

1) ฝ่ายไอซีทีต้องดูแลระบบเครือข่ายของบริษัทฯ ให้เป็นไปอย่างเหมาะสม

2) ฝ่ายไอซีทีต้องตรวจสอบการใช้งาน IP Address ของผู้ใช้งานแต่ละคน และต้องมีการควบคุมการใช้งานที่รัดกุม เพื่อให้สามารถระบุตัวตนบุคคลที่ใช้งานได้ ทั้งนี้ ห้ามใช้งาน หากไม่ใช่ IP Address ที่ได้มาจาก DHCP Server

3) กรณีที่มีการเชื่อมต่อระบบเครือข่ายของบริษัทฯ กับระบบเครือข่ายผ่าน WAN (Wide Area Network) ฝ่ายไอซีทีต้องเข้าใจนโยบายด้านความปลอดภัยทางข้อมูลของมาตรฐานเกี่ยวกับการสร้างระบบเครือข่าย และต้องควบคุมผู้ที่อยู่ภายใต้นโยบายให้ปฏิบัติตามอย่างเคร่งครัด

4) ห้ามใช้ระบบเครือข่าย เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการดำเนินธุรกิจ

5) ต้องใช้งานอย่างเหมาะสม ระมัดระวัง และรอบคอบ เพื่อป้องกันไม่ให้เกิดการรั่วไหลของข้อมูล
6) ไม่ว่าจะด้วยเหตุผลใดก็ตาม ข้อมูลที่ได้รับแจ้ง จะต้องไม่ผ่านการกระทำผิดกฎหมาย เช่น การขโมยข้อมูล เป็นต้น
7) ห้ามเชื่อมต่ออุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนตัว เข้ากับระบบเครือข่ายของบริษัทฯ โดยไม่ได้รับอนุญาตจากฝ่ายไอซีที
8) กรณีที่ระบบสื่อสารสำรองชำรุด ห้ามใช้วิธีการเชื่อมต่อกับระบบเครือข่ายภายนอกด้วยการ Dial up หรือวิธีอื่นๆ ที่นอกเหนือจากสถานการณ์และวิธีการที่เหมาะสมที่ผ่านการเห็นชอบจากฝ่ายไอซีที
9) ห้ามดำเนินการใดๆ ที่ส่งผลให้ความปลอดภัยของระบบเครือข่ายลดลง เช่น การใช้ Tunnel Software
10) ห้ามใช้การสื่อสารใดๆ ที่เป็นการเพิ่มภาระให้แก่ระบบเครือข่าย เช่น ฟังเพลงออนไลน์, ดู YouTube เป็นต้น
11) ห้ามทำ Packet Monitoring หรือการดักดูข้อมูล บนระบบเครือข่าย
12) สำหรับ Windows Shared Disk สามารถดำเนินการได้ตามความเหมาะสมภายในขอบเขตที่ได้รับการอนุญาตจากฝ่ายไอซีที กล่าวคือ ห้ามทำการ Share Disk Drive เช่น C:\
13) ห้ามส่งไฟล์ข้อมูลที่จะส่งผลเสียต่ออุปกรณ์อื่นๆ เช่น ไฟล์ที่มีไวรัส เป็นต้น
14) ข้อห้ามสำหรับการประพฤติปฏิบัติที่พึงระวังต่อการใช้งานระบบเครือข่ายของบริษัทฯ
    - พฤติกรรมอันเป็นการละเมิดลิขสิทธิ์ ได้แก่ การนำเอาข้อความ รูปถ่าย รูปภาพ ข้อมูลอันเป็นงานอันมีลิขสิทธิ์ของบุคคลอื่น เช่น หนังสือ นิตยสาร หนังสือพิมพ์ บทความ โฮมเพจ มาใช้โดยไม่ได้รับอนุญาตหรือโดยมีสิทธิ์ประการอื่น
    - พฤติกรรมอันเป็นการละเมิดลิขสิทธิ์ หรือ เครื่องหมายทางการค้า ได้แก่ การนำเอาตัวอักษรที่ติดไว้ เพื่อแยกแยะสินค้าหรือบริการ มาใช้โดยไม่ได้รับอนุญาต
    - พฤติกรรมอันเป็นการละเมิดลิขสิทธิ์รูป (Image Rights) ได้แก่ การนำเอารูปถ่าย/รูปภาพหน้าตาหรือท่าทางของบุคคลอื่น มาใช้หรือเผยแพร่โดยไม่ได้รับอนุญาต
    - พฤติกรรมอันเป็นการละเมิดลิขสิทธิ์ข้อมูลส่วนบุคคล ได้แก่ การนำเอาข้อมูลส่วนบุคคล ได้แก่ ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ หมายเลขบัตรประจำตัวประชาชน เป็นต้น มาใช้หรือเผยแพร่โดยไม่ได้รับอนุญาต
    - พฤติกรรมอันเป็นการทำลายชื่อเสียง หรือเป็นการหมิ่นประมาท ได้แก่ การเผยแพร่ข้อมูลที่ทำให้บริษัทอื่นเสื่อมเสียชื่อเสียง
    - การเปิดเผยหรือเผยแพร่ข้อความหรือภาพลามก อนาจาร รวมทั้งการแปะลิงค์

15) ห้ามไม่ให้ใช้อุปกรณ์มือถือ หรือแท็บเล็ต เชื่อมต่อเข้ากับระบบเครือข่ายภายใน หากมีความจำเป็นต้องใช้งาน ต้องขออนุญาตจากฝ่ายไอซีที เพื่อดำเนินการลงโปรแกรม Antivirus และโปรแกรมตรวจสอบการทำงานของมือถือ (MDM) ก่อนทำการเชื่อมต่อ

16) ห้ามผู้มาติดต่อภายนอกใช้ระบบเน็ตเวิร์คภายในของบริษัท แต่หากมีความจำเป็นต้องใช้งาน ให้ใช้งานผ่านระบบไวไฟ Pinthong-Guest เพื่อใช้งานอินเตอร์เน็ตได้เท่านั้น (ผ่านการกรอกข้อมูลขอใช้งานในหน้าเว็บไซต์เมื่อมีการเชื่อมต่อ) และกำหนดให้มีอายุการใช้งาน 2 ชั่วโมง (บังคับให้กรอกข้อมูลขอใช้งานใหม่หากครบกำหนด)

5.2) **ระบบอีเมล (E-mail)**

1) ฝ่ายไอซีที ต้องควบคุมดูแลผู้ใช้งาน (User) ของอีเมลอย่างเหมาะสมภายใต้การเห็นชอบจากฝ่ายไอซีที
2) ห้ามมิให้ใช้อีเมล เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการดำเนินธุรกิจ
3) ต้องมีการตั้งรหัสผ่านอย่างเหมาะสม และห้ามบันทึกรหัสผ่านลงในโปรแกรมอีเมล และห้ามใช้ User ของผู้อื่น
4) กรณีที่มีการส่งข้อมูลที่เป็นความลับ ต้องดำเนินการอย่างเหมาะสม และใช้ความระมัดระวังรอบคอบในการส่งข้อมูล
5) กรณีที่มีการตอบกลับ (Reply) หรือส่งต่อ (Forward) อีเมล ต้องพิจารณาอย่างเหมาะสมว่าเนื้อหาของอีเมลนั้นมีส่วนของข้อมูลที่เป็นความลับหรือไม่
6) ต้องรักษามารยาทในการส่งอีเมล ทั้งการส่งอีเมลภายในและภายนอกบริษัท
7) ไฟล์ที่สามารถส่งได้ทางอีเมล มีขนาดใหญ่สุด 130 MB ไม่สามารถส่งไฟล์ที่มีขนาดใหญ่กว่านี้ได้
8) สำหรับไฟล์ที่ถูกส่งมาจากแหล่งที่มาที่ไม่รู้จักหรือน่าสงสัย ให้ลบไฟล์ทิ้งทันที โดยห้ามกระทำการใดๆ กับไฟล์นั้น
9) ฝ่ายไอซีทีจะมีการตรวจสอบรายละเอียดการรับ-ส่งอีเมล โดยไม่ต้องแจ้งล่วงหน้า ซึ่งผู้ที่อยู่ภายใต้นโยบายนี้ รับทราบถึงการตรวจสอบนี้แล้ว

5.3) **ระบบเว็บไซต์ (Website)**

1) ฝ่ายไอซีที ต้องดูแลผู้ใช้งาน (User) ของ Web System อย่างเหมาะสม ภายใต้การเห็นชอบจากผู้จัดการฝ่ายไอซีที
2) ห้ามมิให้ใช้ Web System เพื่อวัตถุประสงค์อื่นที่นอกเหนือจากการดำเนินธุรกิจ
3) ต้องมีการตั้งรหัสผ่านอย่างเหมาะสม และห้ามบันทึกรหัสผ่านลงใน Browser และห้ามใช้ User ของผู้อื่น
4) ต้องใช้ Proxy System ที่เหมาะสม
5) ห้าม Access เข้าเว็บไซต์หรือโฆษณาที่ไม่ปลอดภัย

6) ห้าม Access เข้าเว็บไซต์ทั้งภายในและภายนอกบริษัทฯ เพื่อกระทำการอันเป็นการคุกคามหรือกระทำการอันมีวัตถุประสงค์ที่ไม่สุจริต
7) ห้ามดาวน์โหลดไฟล์ที่ไม่จำเป็นต่อการดำเนินงาน แม้ว่าไฟล์นั้นจะจำเป็นต่อการดำเนินงานก็ไม่อนุญาตให้ Run ไฟล์โดยตรงบน Browser กรณีที่มีการดาวน์โหลดไฟล์ที่จำเป็นต่อการทำงานมานั้น หลังจากดาวน์โหลดไฟล์มาแล้ว จะต้องสแกนไวรัสด้วยทุกครั้ง
8) ฝ่ายไอซีทีจะมีการตรวจสอบรายละเอียดการเข้าถึงเว็บไซต์ โดยไม่ต้องแจ้งล่วงหน้า ซึ่งผู้ที่อยู่ภายใต้นโยบายนี้ รับทราบถึงการตรวจสอบนี้แล้ว
9) ห้ามเข้าใช้บริการเว็บไซต์นอกบริษัทฯ ซึ่งอาจมีการบันทึกข้อมูลของบริษัทฯ ได้
10) ฝ่ายไอซีที จะมีการตรวจสอบการใช้งานคอมพิวเตอร์และระบบเครือข่ายเป็นระยะ
11) ฝ่ายไอซีที ต้องจัดให้มีระบบการลงบันทึก System Log และ Access Log เกี่ยวกับการเข้าถึงข้อมูลต่างๆ ที่มีการเผยแพร่สู่ภายนอก ตลอดจนต้องมีการตรวจสอบเป็นระยะ ว่ามีภัยคุกคามจากการเข้าใช้งานด้วยวัตถุประสงค์ที่ไม่สุจริตหรือไม่
12) ฝ่ายไอซีที ต้องกำหนดกฎระเบียบว่าด้วย การตรวจสอบช่องโหว่ในการดำเนินการตามมาตรการสำหรับเนื้อหา (Content) ที่มีการเผยแพร่สู่ภายนอก และต้องดำเนินการตรวจสอบเป็นระยะ เพื่อรักษาสภาพการใช้งานไม่ให้มีปัญหาช่องโหว่

6. นโยบายการจัดการข้อมูลส่วนบุคคลที่ได้จัดเก็บลงในระบบคอมพิวเตอร์

6.1) ประเภทของข้อมูลที่จัดเก็บ

1) **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลที่เกี่ยวข้องกับการระบุตัวตนของบุคคลธรรมดา บุคคลธรรมดาที่ระบุตัวตนได้ หมายความถึง บุคคลหนึ่งซึ่งสามารถถูกระบุตัวตนได้โดยเฉพาะเจาะจงโดยตรงหรือโดยอ้อม โดยอ้างอิงจากตัวบ่งชี้ใดๆ แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
2) **ข้อมูลระบบ** หมายถึง ข้อมูลที่จัดเก็บเมื่อมีการใช้งานภายใต้โดเมน Pinthongindustrial.com และ Pin-pure.com รวมถึงข้อมูลทางเทคนิค เช่น ที่อยู่ไอพี (IP ADDRESS), ประเภทของ Browser, ประวัติเว็บไซต์ที่เยี่ยมชม, เวลาการเข้าใช้งานเว็บไซต์ , ที่อยู่เว็บไซต์ที่อ้างอิง, ข้อมูลเกี่ยวกับสิ่งที่ค้นหา
3) **ข้อมูลที่ตั้ง** หมายถึง ข้อมูลที่ได้รับจาก GPS, WIFI, เข็มทิศ, ที่อยู่ไอพี (IP ADDRESS), โพสต์สาธารณะ ซึ่งระบุข้อมูลที่ตั้ง
4) **คุ้กกี้เว็บไซต์** หมายถึง ข้อมูลที่ถูกวางในคอมพิวเตอร์ โดย Web Server ซึ่งหลังจากคุ้กกี้ได้ถูกวางในคอมพิวเตอร์ คุ้กกี้จะจัดเก็บและจดจำข้อมูลของผู้ใช้งาน จนกว่าผู้ใช้งานจะปิด Browser นั้น หรือจนกว่าผู้ใช้งานจะลบหรือปฏิเสธคุ้กกี้ อย่างไรก็ตาม จะเป็นการสะดวกต่อการใช้งานเว็บไซต์ได้อย่างง่ายดาย เพราะคุ้กกี้จะช่วยบันทึกและจัดเก็บข้อมูลเว็บไซต์ที่เข้าเยี่ยมชม

5) ข้อมูลอื่น ๆ อาทิ บันทึกภาพและ/หรือเสียงผ่านกล้องวงจรปิด (CCTV) ภาพถ่าย บันทึกภาพและเสียง บันทึกเสียงการสนทนา

6.2) **วัตถุประสงค์ในการนำข้อมูลส่วนบุคคลไปใช้**

1) ข้อมูลส่วนบุคคลที่เกี่ยวกับลูกค้า

ข้อมูลส่วนบุคคลที่เกี่ยวกับลูกค้า ได้แก่ ข้อมูลส่วนบุคคลของลูกค้า (ที่มิใช่ลูกค้าที่เป็นนิติบุคคล) ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ ฝ่ายขาย / ฝ่ายบัญชีและการเงิน

1.1) ใช้เพื่อการจัดส่งข้อมูลการให้บริการและการจัดกิจกรรม
1.2) ใช้เพื่อการให้การสนับสนุนและการบำรุงรักษาเกี่ยวกับอสังหาริมทรัพย์
1.3) ใช้เพื่อการตอบสนองต่อข้อซักถาม และการให้คำปรึกษา
1.4) ใช้เพื่อการออกใบรับรองการให้บริการตามการรับประกัน
1.5) ใช้เพื่อการให้บริการสมาชิกต่างๆ
1.6) ใช้เพื่อการพัฒนาและปรับปรุงเกี่ยวกับอสังหาริมทรัพย์ การทำการสำรวจและจัดทำแบบสอบถามเพื่อดำเนินการตรวจสอบ
1.7) ใช้เพื่อการให้บริการข้อมูล และจัดทำข้อมูลด้านสถิติ
1.8) ใช้เพื่อการตรวจสอบเพื่อวัตถุประสงค์ในการพัฒนาและปรับปรุงกลยุทธ์ทางธุรกิจหรือนโยบายของผู้บริหาร
1.9) ใช้เพื่อการดำเนินงานที่เกี่ยวกับสัญญา
1.10) ใช้เพื่อการเจรจาต่อรองกับลูกค้าในการประชุมอื่น
1.11) ใช้เพื่อการให้ข้อมูลที่เป็นประโยชน์ต่อลูกค้าของบริษัทฯ

2) ข้อมูลส่วนบุคคลที่เกี่ยวกับผู้ถือหุ้น

ข้อมูลส่วนบุคคลที่เกี่ยวกับผู้ถือหุ้น ได้แก่ ข้อมูลส่วนบุคคลของผู้ถือหุ้น ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ เลขานุการบริษัท หรือ นายทะเบียนบริษัทฯ

2.1) ใช้เพื่อการดำเนินการใช้สิทธิและหน้าที่ตามกฎหมายและข้อบังคับของบริษัท
2.2) ใช้เพื่อความสะดวกต่อการใช้งาน เช่น เอกสารแสดงเงินปันผลที่ผู้ถือหุ้นจะได้รับเป็นต้น
2.3) ใช้เพื่อดำเนินการตามมาตรการต่างๆ ของผู้ถือหุ้น เช่น แบบสอบถาม
2.4) ใช้เพื่อการบริหารจัดการข้อมูลของผู้ถือหุ้นตามกฎหมายและกฎระเบียบ เช่น การสร้างข้อมูลผู้ถือหุ้น

3) ข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าหน้าที่ / พนักงานของบริษัท / นักศึกษาฝึกงาน

ข้อมูลส่วนบุคคลที่เกี่ยวกับเจ้าหน้าที่/พนักงานของบริษัท/นักศึกษาฝึกงาน ได้แก่ ข้อมูลส่วนบุคคลของพนักงาน และผู้มาติดต่อขอสมัครงาน รวมถึงข้อมูลส่วนบุคคลของนักศึกษาฝึกงาน ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ ฝ่ายทรัพยากรบุคคลและธุรการ

3.1) ใช้เพื่อการติดต่อสื่อสารและเจรจาต่อรอง เพื่อการดำเนินงานของบริษัทฯ

3.2) ใช้เพื่อการจัดการและประมวลผล ข้อมูลรายได้และการจ่ายเงินเดือน ค่าตอบแทน หรือ สิทธิประโยชน์อื่นใดให้เจ้าหน้าที่/พนักงานของบริษัท/นักศึกษาฝึกงาน

4) ข้อมูลส่วนบุคคลที่เกี่ยวกับผู้จำหน่าย/ผู้รับเหมา (Supplier)

ข้อมูลส่วนบุคคลที่เกี่ยวกับผู้จำหน่าย/ผู้รับเหมา (Supplier) ได้แก่ ข้อมูลส่วนบุคคลของผู้จำหน่าย/ผู้รับเหมา (Supplier) ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ ฝ่ายจัดซื้อจัดจ้าง / ฝ่ายบัญชีและการเงิน

4.1) ใช้เพื่อตรวจสอบข้อมูล คุณสมบัติ และดำเนินการวิธีการจัดซื้อ จัดจ้าง ของบริษัทฯ

4.2) ใช้เพื่อการดำเนินงานที่เกี่ยวกับสัญญา และงานที่ได้รับมอบหมาย

4.3) ใช้เพื่อการชำระราคาและการดำเนินการที่เกี่ยวกับด้านบัญชีและการเงิน

5) ข้อมูลส่วนบุคคลที่เกี่ยวกับการจ้างงานพนักงาน

ข้อมูลส่วนบุคคลที่เกี่ยวกับการจ้างงานพนักงาน ได้แก่ ข้อมูลส่วนบุคคลของพนักงาน และผู้สมัครงาน ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ ฝ่ายทรัพยากรบุคคลและธุรการ

5.1) ใช้เพื่อเป็นข้อมูลในการติดต่อสมัครงาน และประกอบการพิจารณาคัดเลือกพนักงานที่เหมาะสมกับงาน

5.2) ใช้เพื่อการบริหารจัดการการดำเนินงานของบริษัทฯ และเรื่องที่เกี่ยวข้อง

5.3) ใช้เพื่อการติดต่อสื่อสารกับพนักงานที่ลาออกจากบริษัทฯ ไปแล้ว

6) ข้อมูลอื่น ๆ เพื่อรักษาความมั่นคงปลอดภัยของบริษัทฯ

ข้อมูลอื่นๆ อาทิ บันทึกภาพและ/หรือเสียงผ่านกล้องวงจรปิด (CCTV) ภาพถ่าย บันทึกภาพและเสียง บันทึกเสียงการสนทนา ซึ่งผู้ใช้ข้อมูลหลักและผู้ประมวลผลข้อมูลดังกล่าว คือ ฝ่ายไอซีที และ ฝ่ายพื้นที่ส่วนกลาง

6.1) เพื่อตรวจสอบข้อมูลการใช้บริการของบริษัทฯ ในการพัฒนามาตรฐานความมั่นคงปลอดภัยในการให้บริการ การจัดการและการคุ้มครองโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ

6.2) เพื่อควบคุมการเข้าออกอาคาร และเพื่อทำให้มั่นใจว่าอาคารและพื้นที่ของบริษัทฯ มีความปลอดภัยและความมั่นคงต่อบุคลากรของบริษัทฯ รวมทั้งต่อทรัพย์สินและข้อมูลต่างๆ ที่ตั้งอยู่หรือจัดเก็บในอาคาร เพื่อเฝ้าสังเกตและตรวจตราการเข้าออกอาคาร สถานที่ที่มีการรักษาความปลอดภัย ห้องที่มีการป้องกัน โครงสร้างพื้นฐาน

เกี่ยวกับเทคโนโลยีสารสนเทศหรือข้อมูลเชิงปฏิบัติการ และพื้นที่อื่น (รวมเรียกว่า "อาคารและพื้นที่") ซึ่งเป็นการป้องกันการเข้าออกอาคารและพื้นที่ของบริษัทฯ โดยไม่ได้รับอนุญาต และเพื่อป้องกัน ตรวจจับ และสืบสวนเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย เช่น การเข้าออกอาคารและพื้นที่ของบริษัทฯ โดยไม่ได้รับอนุญาต การโจรกรรม อัคคีภัย หรือการทำร้ายร่างกาย

6.3) **การเปิดเผยข้อมูลส่วนบุคคล**

บริษัทฯ อาจเปิดเผยข้อมูลส่วนบุคคลดังกล่าวมาแล้วข้างต้น ภายใต้วัตถุประสงค์ที่กำหนดและตามหลักเกณฑ์ที่กฎหมายกำหนดแก่หน่วยงานและบุคคล ดังต่อไปนี้

(1) บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน) และ กลุ่มบริษัทปิ่นทอง และให้หมายความรวมถึงพนักงาน ลูกจ้าง กรรมการ ผู้จัดการ หรือบุคลากรของบริษัทฯ เท่าที่เกี่ยวข้องและตามจำเป็นเพื่อการประมวลผลข้อมูลส่วนบุคคล

(2) หน่วยงานของรัฐ หน่วยงานที่มีหน้าที่กำกับดูแลตามกฎหมาย

(3) หน่วยงานที่ร้องขอให้เปิดเผยข้อมูลโดยอาศัยอำนาจตามกฎหมาย

(4) พันธมิตร คู่ค้าธุรกิจ ผู้ให้บริการ ผู้รับบริการ และผู้ประมวลผลข้อมูลส่วนบุคคลที่บริษัทฯ มอบหมายให้ทำหน้าที่ดูแลรับผิดชอบ หรือบริหารจัดการเกี่ยวกับข้อมูลส่วนบุคคล อาทิ ด้านการพัฒนาปรับปรุง หรือดูแลรักษามาตรฐานความมั่นคงปลอดภัยของระบบงานและระบบเทคโนโลยีสารสนเทศ ด้านระบบการชำระเงิน การตรวจสอบทางบัญชี การบริหารจัดการทรัพยากรบุคคล

(5) การเปิดเผยข้อมูลส่วนบุคคล (กรณีที่ไม่ใช่นิติบุคคล) ให้กับบุคคลอื่น จะดำเนินการภายใต้วัตถุประสงค์ที่กำหนด หรือวัตถุประสงค์อื่นที่กฎหมายกำหนดให้กระทำได้เท่านั้น ในกรณีที่กฎหมายกำหนดว่าต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล บริษัทฯ จะขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อนทุกครั้ง

(6) ในกรณีที่บริษัทฯ เปิดเผยข้อมูลส่วนบุคคล (กรณีที่ไม่ใช่นิติบุคคล) ให้กับบุคคลอื่น บริษัทฯ จะจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลที่ได้เปิดเผยและเพื่อปฏิบัติตามมาตรฐานและหน้าที่การคุ้มครองข้อมูลส่วนบุคคล ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

6.4) **ความยินยอมและสิทธิเกี่ยวกับข้อมูล**

การจัดเก็บ การใช้ หรือการเผยแพร่ข้อมูลส่วนบุคคล บริษัทฯ จะต้องขอความยินยอมโดยตรงจากเจ้าของข้อมูลก่อนหรือในขณะดำเนินการทุกครั้ง โดยในการให้ความยินยอมนั้น จะกระทำเป็นหนังสือ แบบฟอร์ม หรือวิธีการที่บริษัทฯ กำหนด ทั้งนี้ เจ้าของข้อมูลมีสิทธิเกี่ยวกับข้อมูลดังนี้

1) **สิทธิในการเข้าถึงข้อมูล** เพื่อรับทราบข้อมูลส่วนบุคคลที่ได้รับการจัดเก็บ

2) **สิทธิในการแก้ไขข้อมูลให้ถูกต้องและเป็นปัจจุบัน** กรณีที่ข้อมูลส่วนบุคคลไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่เป็นปัจจุบัน เจ้าของข้อมูลมีสิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง และเป็นปัจจุบัน

3) **สิทธิในการแจ้งลบข้อมูล** กรณีที่เป็นข้อมูลที่ไม่มีความจำเป็นต่อวัตถุประสงค์ในการจัดเก็บหรือประมวลผลอีกต่อไป หรือกรณีที่เจ้าของข้อมูลแจ้งถอนความยินยอมฯ หรือกรณีที่การประมวลผลข้อมูลนั้น ไม่ชอบด้วยกฎหมาย เจ้าของข้อมูลมีสิทธิแจ้งลบข้อมูลนั้นได้

6.5) **ระยะเวลาในการเก็บรักษาข้อมูล**

1) ข้อมูลส่วนบุคคลที่เกี่ยวกับพนักงานและผู้มาสมัครงาน จัดเก็บตลอดระยะเวลาการเป็นพนักงาน

2) ข้อมูลส่วนบุคคลที่เกี่ยวกับผู้จำหน่าย/ผู้รับเหมา(Supplier) จัดเก็บตลอดระยะเวลาการเป็นคู่ค้า

3) ข้อมูลส่วนบุคคลที่เกี่ยวกับลูกค้า (ที่มิใช่ลูกค้าที่เป็นนิติบุคคล) จัดเก็บตลอดระยะเวลาการเป็นคู่ค้า

6.6) **การปฏิบัติตามนโยบายการจัดการข้อมูลส่วนบุคคลที่ได้จัดเก็บลงในระบบคอมพิวเตอร์** ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง และให้หมายความรวมถึงกฎหมายฉบับแก้ไขเพิ่มเติมใดๆ ในอนาคต รวมถึงนโยบายคุ้มครองข้อมูลส่วนบุคคล และแนวทางการจัดการข้อมูลส่วนบุคคล (PDPA) บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน) ฉบับลงวันที่ วันที่ 25 กุมภาพันธ์ 2565 หรือที่มีการแก้ไขปรับปรุงนโยบายฯ ในอนาคต

7. การควบคุมดูแลการว่าจ้างผู้ให้บริการดูแลระบบ

7.1) **การคัดเลือกผู้ให้บริการดูแลระบบ**

กรณีที่จะว่าจ้างผู้ให้บริการดูแลระบบ ต้องเลือกผู้ให้บริการดูแลระบบที่น่าเชื่อถือ และสามารถดำเนินงานตามขอบเขตงานที่กำหนดได้

7.2) **การทำสัญญากับผู้ให้บริการดูแลระบบ**

การทำสัญญาหรือทำข้อตกลงเป็นลายลักษณ์อักษร จะต้องมีการระบุข้อความอันเป็นข้อความที่เกี่ยวกับการรักษาความปลอดภัยของข้อมูล ดังนี้

1) การปฏิบัติตามนโยบายรักษาความปลอดภัยของข้อมูลของบริษัทฯ อย่างเคร่งครัด

2) การรักษาข้อมูลที่เป็นความลับ

- ห้ามเปิดเผยหรือเผยแพร่ข้อมูลที่ได้รับมา ให้แก่บุคคลที่สาม โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบอำนาจดำเนินการนั้น

3) การควบคุมดูแลข้อมูลอย่างเหมาะสม

- การระบุตัวตนของบุคคลที่เป็นผู้มีหน้าที่รับผิดชอบข้อมูลให้ชัดเจน เช่น ผู้จัดการฝ่ายของบริษัทผู้ให้บริการดูแลระบบ

- การควบคุมดูแลข้อมูลอย่างเหมาะสม และป้องกันไม่ให้เกิดการสูญหาย การรั่วไหล และการเปลี่ยนแปลงข้อมูล
- กรณีที่มีการส่งมอบอุปกรณ์จัดเก็บและบันทึกข้อมูล ต้องทำการสแกนไวรัสทุกครั้ง

4) บทลงโทษ กรณีที่ไม่ปฏิบัติตามสัญญา

- กรณีที่ไม่ปฏิบัติตามสัญญา ต้องมีมาตรการในการดำเนินการ เช่น เรียกร้องค่าเสียหาย ฯลฯ

7.3) การควบคุมการเข้าดำเนินงานของผู้ให้บริการดูแลระบบ

1) ผู้ให้บริการดูแลระบบ ที่รีโมทเข้าดำเนินงานแก้ไข ปรับปรุงระบบ ตามที่ได้รับการว่าจ้าง ต้องแจ้งขออนุญาตเข้าดำเนินการ และแจ้งขอรหัสผ่าน สำหรับเชื่อมต่อ VPN เข้าสู่ระบบ โดยส่งอีเมลแจ้งเรื่องดังกล่าวมายังฝ่ายไอซีที เพื่อพิจารณาตามความเหมาะสม
2) รหัสผ่าน (Password) เพื่อให้ผู้ให้บริการดูแลระบบ Log in ในการเชื่อมต่อ VPN เข้าใช้งาน จะมีอายุการใช้งานไม่เกิน 48 ชั่วโมงเท่านั้น

8. ข้อควรระวังเกี่ยวกับระบบสารสนเทศ

ควรดำเนินการตามมาตรการทางกายภาพที่สำคัญ เช่น

- การจัดเก็บ Server Rack และการติดตั้งห้อง Server แยกออกมา
- มาตรการรองรับกรณีเกิดเหตุฉุกเฉิน เช่น แผ่นดินไหว ไฟดับ ไฟไหม้ ระบบปรับอากาศ ระบบไฟฟ้า และการวางสายไฟ เป็นต้น
- มาตรการควบคุมการเข้าถึงห้อง Server ได้แก่ การจำกัดสิทธิในการเข้าห้อง Server, การบันทึกการเข้า-ออกห้อง Server, และการตรวจสอบการบันทึกการเข้า-ออกห้อง Server

8.1) **Core System** ควรมีการสำรองข้อมูลเป็นประจำ และตรวจสอบผลการสำรองข้อมูลสม่ำเสมอ

8.2) **File Server** ควรมีการสำรองข้อมูลไว้มากกว่า 1 Media เพื่อสำรองไว้ใช้กรณีที่ข้อมูลเกิดความเสียหาย

8.3) **Mail System**

- มีการเก็บรักษาประวัติการรับ-ส่งอีเมล อย่างน้อย 90 วัน
- ผู้ใช้งาน (User) ควรทำ Mail Archive เพื่อจัดเก็บอีเมลที่รับ-ส่งไว้ อย่างน้อย 90 วัน

8.4) **Proxy System** ควรมีการจัดเก็บบันทึกประวัติการเข้าชมเว็บไซต์นอกบริษัทฯ อย่างน้อย 90 วัน ตามที่กฎหมายกำหนดไว้

9. การควบคุมบัญชีผู้ใช้งาน

9.1) การลงทะเบียนสร้างบัญชีผู้ใช้งาน (Create Account)

แจ้งขอลงทะเบียนเปิดบัญชีผู้ใช้งาน (Create Account) ผ่านระบบ IT Care เพื่อให้ฝ่ายไอซีทีดำเนินการตามที่หน่วยงานแจ้งคำขอ โดยฝ่ายไอซีทีต้องตรวจสอบมิให้มีการสร้างบัญชีผู้ใช้งานร่วมกัน

9.2) **การลบ**

แจ้งลบบัญชีผู้ใช้งาน (Delete Account) ที่ไม่ใช้งานแล้ว สำหรับกรณีที่มีการโอนย้ายพนักงาน หรือกรณีที่พนักงานลาออก ฝ่ายไอซีทีต้องมีตรวจสอบเอกสารประกอบการแจ้งลบบัญชีผู้ใช้งานจากฝ่ายทรัพยากรบุคคลและธุรการให้ครบถ้วน ก่อนที่จะดำเนินการลบบัญชีผู้ใช้งานนั้น หรือปิดการใช้งานของบัญชีผู้ใช้งานนั้นได้ หลังจากลบหรือปิดบัญชีผู้ใช้งานนั้นแล้ว ฝ่ายไอซีทีต้องเก็บบัญชีนั้นไว้ก่อน อย่างน้อย 90 วัน จึงจะสามารถลบบัญชีผู้ใช้งานนั้นออกจากระบบได้

9.3) **การแก้ไขหรือการเปลี่ยนแปลง**

แจ้งให้ดำเนินการแก้ไขหรือเปลี่ยนแปลงข้อมูลของบัญชีผู้ใช้งาน ผ่านระบบ IT Care เพื่อให้ฝ่ายไอซีที ดำเนินการตามที่หน่วยงานแจ้งคำขอ

10. การดำเนินการเกี่ยวกับเหตุการณ์ที่เกิดขึ้นโดยไม่คาดคิด

10.1) **เมื่อเกิดเหตุการณ์**

กรณีที่เกิดเหตุการณ์ร้ายแรง ไม่ว่าจะส่งผลกระทบต่อระบบหรือไม่ ไม่ว่าจะส่งผลกระทบทั้งทางตรงหรือทางอ้อมก็ตาม ฝ่ายไอซีทีต้องดำเนินการจดบันทึก Incident Report เพื่อรายงานเหตุการณ์ที่เกิดขึ้นทุกเหตุการณ์นั้น พร้อมชี้แจงขั้นตอนการเข้าดำเนินการแก้ไขปัญหา และวิเคราะห์แนวทางการแก้ไขปัญหา เพื่อป้องกันมิให้เกิดเหตุการณ์ซ้ำ

10.2) **แผนการป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ**

ฝ่ายไอซีที ต้องทำการวิเคราะห์และกำหนดมาตรการเพื่อป้องกันการเกิดเหตุการณ์ซ้ำ

10.3) **แผนการดำเนินการเมื่อเกิดเหตุการณ์ฉุกเฉิน**

จัดให้มีการซักซ้อมแผน และทบทวนเพื่อปรับปรุงแก้ไข "แผนความต่อเนื่องทางธุรกิจ" อย่างน้อยปีละ 1 ครั้ง เพื่อเตรียมความพร้อมและซักซ้อมแผนการเข้าดำเนินการกู้คืนระบบอย่างสม่ำเสมอ

11. อื่น ๆ

11.1) **การปฏิบัติตามกฎหมาย**

นอกเหนือจากกฎระเบียบที่กำหนดไว้ในนโยบายนี้แล้ว ผู้ที่อยู่ภายใต้นโยบายฯ จะต้องปฏิบัติตามกฎหมายของประเทศไทย และกฎระเบียบในการปฏิบัติงานของบริษัทฯ อย่างเคร่งครัด

11.2) **การรายงาน**

กรณีที่เกิดเหตุการณ์ที่เป็นการขัดต่อเนื้อหาที่กำหนดไว้ในนโยบายนี้ หรือกรณีที่มีการดำเนินการในสิ่งที่ขัดต่อนโยบายนี้ หรือพบเห็นพฤติกรรมของผู้ที่อยู่ภายใต้นโยบายนี้ ต้องแจ้งรายงานต่อฝ่ายไอซีทีทันที

11.3) **การตรวจสอบ**

ฝ่ายไอซีที ต้องวางแผนการตรวจสอบการปฏิบัติตามนโยบายนี้ ให้มีการดำเนินการตรวจติดตามสม่ำเสมอ และประเมินความเหมาะสมของนโยบายนี้ พร้อมทั้งต้องพิจารณาทบทวนการแก้ไขนโยบายนี้ตามความจำเป็น

11.4) บทลงโทษ

กรณีที่ผู้ที่อยู่ภายใต้นโยบายนี้ กระทำการใดๆ ที่ขัดต่อนโยบายนี้ อาจมีการพิจารณายกเลิกบัญชีผู้ใช้งานนั้น และพิจารณาดำเนินการลงโทษทางวินัยตามระเบียบข้อบังคับของบริษัทฯ ตามความเหมาะสม หรืออาจพิจารณาให้ดำเนินคดีตามกฎหมายต่อไป

11.5) การชดใช้ความเสียหาย

กรณีที่ผู้ที่อยู่ภายใต้นโยบายนี้ กระทำการใดๆ ที่ขัดต่อนโยบายนี้ อันเป็นความผิดที่ร้ายแรง ไม่ว่าจะเป็นการกระทำโดยเจตนาหรือไม่ก็ตาม หากบริษัทฯ ได้รับความเสียหายอย่างใหญ่หลวง อาจมีการเรียกร้องให้ผู้ที่กระทำความผิด ชดใช้ความเสียหายนั้น

11.6) การศึกษา การฝึกอบรม และการให้ความรู้

ฝ่ายไอซีที ต้องให้ความรู้ด้านเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน (User) ที่ใช้งานทรัพย์สินด้านสารสนเทศ โดยอาจจะจัดให้มีการฝึกอบรม และต้องจัดทำรายงานการฝึกอบรมที่มีข้อมูลวันที่ฝึกอบรม รายชื่อผู้เข้าร่วมการอบรม เนื้อหาการฝึกอบรม หรือการให้ความรู้ผ่านช่องทางต่างๆ เช่น อีเมล ภาพแบ็คกราวของหน้าจอคอมพิวเตอร์ เป็นต้น

11.7) การแก้ไข

ผู้ที่มีความประสงค์ให้มีการปรับเปลี่ยนนโยบายนี้ จะต้องยื่นเรื่องแจ้งความประสงค์ต่อฝ่ายไอซีที เพื่อพิจารณาให้มีการเปลี่ยนแปลง โดยนโยบายนี้ จะมีการพิจารณาทบทวนการแก้ไขปีละ 1 ครั้ง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับแก้ไขครั้งที่ 6 นี้ มีผลใช้บังคับตั้งแต่วันที่ 13 พฤศจิกายน 2567 โดยการอนุมัติของคณะกรรมการบริษัท ครั้งที่ 4/2567

(นายประสาน ตันประเสริฐ)
ประธานกรรมการบริษัท
บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน)

ภาคผนวก ก.รายละเอียดยูสเซอร์เนมระบบงาน ERP

Linux ERPPROD และ ERPPRODDB

NO.	USER	Server	Password Policy
1	root	ERPPROD, ERPPRODDB	90 DAYS
2	sarunyou	ERPPROD, ERPPRODDB	90 DAYS
3	teerawit	ERPPROD, ERPPRODDB	90 DAYS
4	abrt	ERPPROD, ERPPRODDB	NO
5	adm	ERPPROD, ERPPRODDB	NO
6	applprod	ERPPROD, ERPPRODDB	NO
7	avahi	ERPPROD, ERPPRODDB	NO
8	avahi-autoipd	ERPPROD, ERPPRODDB	NO
9	bin	ERPPROD, ERPPRODDB	NO
10	chrony	ERPPROD, ERPPRODDB	NO
11	colord	ERPPROD, ERPPRODDB	NO
12	daemon	ERPPROD, ERPPRODDB	NO
13	dbus	ERPPROD, ERPPRODDB	NO
14	ftp	ERPPROD, ERPPRODDB	NO

15	games	ERPPROD, ERPPRODDB	NO
16	gdm	ERPPROD, ERPPRODDB	NO
17	geoclue	ERPPROD, ERPPRODDB	NO
18	gnome-initial-setup	ERPPROD, ERPPRODDB	NO
19	halt	ERPPROD, ERPPRODDB	NO
20	libstoragemgmt	ERPPROD, ERPPRODDB	NO
21	lp	ERPPROD, ERPPRODDB	NO
22	mail	ERPPROD, ERPPRODDB	NO
23	nfsnobody	ERPPROD, ERPPRODDB	NO
24	nobody	ERPPROD, ERPPRODDB	NO
25	ntp	ERPPROD, ERPPRODDB	NO
26	operator	ERPPROD, ERPPRODDB	NO
27	oracle	ERPPROD, ERPPRODDB	NO
28	polkitd	ERPPROD, ERPPRODDB	NO
29	postfix	ERPPROD, ERPPRODDB	NO
30	pulse	ERPPROD, ERPPRODDB	NO
31	qemu	ERPPROD, ERPPRODDB	NO

32	radvd	ERPPROD, ERPPRODDB	NO
33	rpc	ERPPROD, ERPPRODDB	NO
34	rpcuser	ERPPROD, ERPPRODDB	NO
35	rtkit	ERPPROD, ERPPRODDB	NO
36	saslauth	ERPPROD, ERPPRODDB	NO
37	setroubleshoot	ERPPROD, ERPPRODDB	NO
38	shutdown	ERPPROD, ERPPRODDB	NO
39	sshd	ERPPROD, ERPPRODDB	NO
40	sync	ERPPROD, ERPPRODDB	NO
41	systemd-bus-proxy	ERPPROD, ERPPRODDB	NO
42	systemd-network	ERPPROD, ERPPRODDB	NO
43	tcpdump	ERPPROD, ERPPRODDB	NO
44	tss	ERPPROD, ERPPRODDB	NO
45	unbound	ERPPROD, ERPPRODDB	NO
46	upload	ERPPROD	NO
47	usbmuxd	ERPPROD, ERPPRODDB	NO

ORACLE DB

NO.	USER	System	Password Policy
1	SYS	ORACLE DB	90 DAYS
2	SYSTEM	ORACLE DB	90 DAYS
3	AD_MONITOR	ORACLE DB	NO
4	AHL	ORACLE DB	NO
5	AK	ORACLE DB	NO
6	ALR	ORACLE DB	NO
7	AMS	ORACLE DB	NO
8	AMV	ORACLE DB	NO
9	ANONYMOUS	ORACLE DB	NO
10	AP	ORACLE DB	NO
11	APPLSYS	ORACLE DB	NO
12	APPLSYSPUB	ORACLE DB	NO
13	APPQOSSYS	ORACLE DB	NO
14	APPS	ORACLE DB	NO
15	APPS_NE	ORACLE DB	NO
16	AR	ORACLE DB	NO
17	ASF	ORACLE DB	NO
18	ASG	ORACLE DB	NO
19	ASL	ORACLE DB	NO
20	ASN	ORACLE DB	NO
21	ASO	ORACLE DB	NO
22	ASP	ORACLE DB	NO
23	AST	ORACLE DB	NO
24	AUDSYS	ORACLE DB	NO
25	AX	ORACLE DB	NO
26	AZ	ORACLE DB	NO
27	BEN	ORACLE DB	NO
28	BIC	ORACLE DB	NO
29	BIM	ORACLE DB	NO
30	BIS	ORACLE DB	NO

31	BNE	ORACLE DB	NO
32	BOM	ORACLE DB	NO
33	CCT	ORACLE DB	NO
34	CE	ORACLE DB	NO
35	CLA	ORACLE DB	NO
36	CLN	ORACLE DB	NO
37	CMI	ORACLE DB	NO
38	CN	ORACLE DB	NO
39	CRP	ORACLE DB	NO
40	CS	ORACLE DB	NO
41	CSC	ORACLE DB	NO
42	CSD	ORACLE DB	NO
43	CSE	ORACLE DB	NO
44	CSF	ORACLE DB	NO
45	CSI	ORACLE DB	NO
46	CSL	ORACLE DB	NO
47	CSM	ORACLE DB	NO
48	CSP	ORACLE DB	NO
49	CSR	ORACLE DB	NO
50	CTXSYS	ORACLE DB	NO
51	CUA	ORACLE DB	NO
52	CUG	ORACLE DB	NO
53	CZ	ORACLE DB	NO
54	DBSNMP	ORACLE DB	NO
55	DDR	ORACLE DB	NO
56	DIP	ORACLE DB	NO
57	DNA	ORACLE DB	NO
58	DOM	ORACLE DB	NO
59	DPP	ORACLE DB	NO
60	EAM	ORACLE DB	NO
61	EC	ORACLE DB	NO
62	ECX	ORACLE DB	NO
63	EDR	ORACLE DB	NO
64	EGO	ORACLE DB	NO

65	EM_MONITOR	ORACLE DB	NO
66	ENG	ORACLE DB	NO
67	ENI	ORACLE DB	NO
68	FA	ORACLE DB	NO
69	FLM	ORACLE DB	NO
70	FPA	ORACLE DB	NO
71	FRM	ORACLE DB	NO
72	FTE	ORACLE DB	NO
73	FUN	ORACLE DB	NO
74	FV	ORACLE DB	NO
75	GHG	ORACLE DB	NO
76	GL	ORACLE DB	NO
77	GMA	ORACLE DB	NO
78	GMD	ORACLE DB	NO
79	GME	ORACLE DB	NO
80	GMF	ORACLE DB	NO
81	GMI	ORACLE DB	NO
82	GML	ORACLE DB	NO
83	GMO	ORACLE DB	NO
84	GMP	ORACLE DB	NO
85	GMS	ORACLE DB	NO
86	GR	ORACLE DB	NO
87	GSMADMIN_INTERNAL	ORACLE DB	NO
88	GSMCATUSER	ORACLE DB	NO
89	GSMUSER	ORACLE DB	NO
90	HR	ORACLE DB	NO
91	HRI	ORACLE DB	NO
92	HXC	ORACLE DB	NO
93	HXT	ORACLE DB	NO
94	IA	ORACLE DB	NO
95	IBC	ORACLE DB	NO
96	IBE	ORACLE DB	NO
97	IBU	ORACLE DB	NO
98	IBW	ORACLE DB	NO

99	IBY	ORACLE DB	NO
100	ICX	ORACLE DB	NO
101	IEB	ORACLE DB	NO
102	IEC	ORACLE DB	NO
103	IEM	ORACLE DB	NO
104	IEO	ORACLE DB	NO
105	IES	ORACLE DB	NO
106	IEU	ORACLE DB	NO
107	IEX	ORACLE DB	NO
108	IGC	ORACLE DB	NO
109	IGI	ORACLE DB	NO
110	IMC	ORACLE DB	NO
111	INL	ORACLE DB	NO
112	INV	ORACLE DB	NO
113	IPA	ORACLE DB	NO
114	IPM	ORACLE DB	NO
115	ITG	ORACLE DB	NO
116	IZU	ORACLE DB	NO
117	JA	ORACLE DB	NO
118	JE	ORACLE DB	NO
119	JG	ORACLE DB	NO
120	JL	ORACLE DB	NO
121	JMF	ORACLE DB	NO
122	JTF	ORACLE DB	NO
123	JTM	ORACLE DB	NO
124	LNS	ORACLE DB	NO
125	MDDATA	ORACLE DB	NO
126	MDSYS	ORACLE DB	NO
127	MFG	ORACLE DB	NO
128	MGDSYS	ORACLE DB	NO
129	MRP	ORACLE DB	NO
130	MSC	ORACLE DB	NO
131	MSD	ORACLE DB	NO
132	MSO	ORACLE DB	NO

133	MSR	ORACLE DB	NO
134	MTH	ORACLE DB	NO
135	MWA	ORACLE DB	NO
136	ODM	ORACLE DB	NO
137	ODM_MTR	ORACLE DB	NO
138	OE	ORACLE DB	NO
139	OJVMSYS	ORACLE DB	NO
140	OKC	ORACLE DB	NO
141	OKE	ORACLE DB	NO
142	OKL	ORACLE DB	NO
143	OKS	ORACLE DB	NO
144	OKX	ORACLE DB	NO
145	OLAPSYS	ORACLE DB	NO
146	ONT	ORACLE DB	NO
147	OPI	ORACLE DB	NO
148	ORACLE_OCM	ORACLE DB	NO
149	ORDDATA	ORACLE DB	NO
150	ORDPLUGINS	ORACLE DB	NO
151	ORDSYS	ORACLE DB	NO
152	OSM	ORACLE DB	NO
153	OTA	ORACLE DB	NO
154	OUTLN	ORACLE DB	NO
155	OZF	ORACLE DB	NO
156	PA	ORACLE DB	NO
157	PJI	ORACLE DB	NO
158	PJM	ORACLE DB	NO
159	PMI	ORACLE DB	NO
160	PN	ORACLE DB	NO
161	PO	ORACLE DB	NO
162	POM	ORACLE DB	NO
163	PON	ORACLE DB	NO
164	POS	ORACLE DB	NO
165	PRP	ORACLE DB	NO
166	PSA	ORACLE DB	NO

167	PSP	ORACLE DB	NO
168	PV	ORACLE DB	NO
169	QA	ORACLE DB	NO
170	QOT	ORACLE DB	NO
171	QP	ORACLE DB	NO
172	QPR	ORACLE DB	NO
173	QRM	ORACLE DB	NO
174	RG	ORACLE DB	NO
175	RLM	ORACLE DB	NO
176	RRS	ORACLE DB	NO
177	SCOTT	ORACLE DB	NO
178	SI_INFORMTN_SCHEMA	ORACLE DB	NO
179	SPATIAL_CSW_ADMIN_USR	ORACLE DB	NO
180	SPATIAL_WFS_ADMIN_USR	ORACLE DB	NO
181	SSOSDK	ORACLE DB	NO
182	SSP	ORACLE DB	NO
183	SYSBACKUP	ORACLE DB	NO
184	SYSDG	ORACLE DB	NO
185	SYSKM	ORACLE DB	NO
186	TEERAWIT	ORACLE DB	NO
187	VEA	ORACLE DB	NO
188	WIP	ORACLE DB	NO
189	WMS	ORACLE DB	NO
190	WPS	ORACLE DB	NO
191	WSH	ORACLE DB	NO
192	WSM	ORACLE DB	NO
193	XCUST	ORACLE DB	NO
194	XDB	ORACLE DB	NO
195	XDO	ORACLE DB	NO
196	XDP	ORACLE DB	NO
197	XLA	ORACLE DB	NO
198	XLE	ORACLE DB	NO
199	XNB	ORACLE DB	NO
200	XNP	ORACLE DB	NO

201	XPN	ORACLE DB	NO
202	XS$NULL	ORACLE DB	NO
203	XTR	ORACLE DB	NO
204	YMS	ORACLE DB	NO
205	ZX	ORACLE DB	NO