**นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน**
**(Governance Risk Compliance : GRC) ประจำปีงบประมาณ พ.ศ. 2569**

**GRC (Governance, Risk Management, and Compliance)** เป็นกลยุทธ์ในการดำเนินงานเพื่อขับเคลื่อนองค์กรไปสู่การบริหารองค์กรแบบบูรณาการอย่างมีคุณค่า (Business Integrity) และการมีคุณธรรมในการบริหาร เช่น การกำหนดกฎเกณฑ์ ระเบียบคำสั่ง และการปฏิบัติ การให้คุณให้โทษ จะต้องมี ความชัดเจน สอดคล้องกันทั่วทั้งองค์กรในทุกมุมมองของการบริหารตามหลัก Balanced Scorecards และมีการปฏิบัติอย่างจริงจัง รวมถึงผู้บริหารทุกระดับมีหน้าที่ปลูกฝังจิตสำนึกด้านการบริหารความเสี่ยงและการควบคุมภายในปรับเปลี่ยนวัฒนธรรมขององค์กร ให้แก่พนักงานและลูกจ้างของบริษัท อู่กรุงเทพ จำกัด เพื่อสร้างเป็นวัฒนธรรมในการทำงานไปสู่วัตถุประสงค์และเป้าหมายด้านวัฒนธรรมองค์กรที่คาดหวังเพื่อเพิ่มประสิทธิภาพ สนับสนุนหรือผลักดันให้การดำเนินงานขององค์กรบรรลุตามวัตถุประสงค์ได้ดีขึ้น

บริษัท อู่กรุงเทพ จำกัด ได้กำหนด วิสัยทัศน์ของการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน ไว้ดังนี้ “พัฒนาองค์กรให้มีระบบการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายในแบบบูรณาการ เพื่อสร้างความยั่งยืนและเพิ่มมูลค่าองค์กร”

**1. บทนำและวัตถุประสงค์**

เอกสารฉบับนี้จัดทำขึ้นเพื่อทบทวนและปรับปรุงนโยบายกำกับดูแลกิจการที่ดี (Governance), การบริหารความเสี่ยง (Risk Management) และการควบคุมภายในและการปฏิบัติตามข้อกำหนด (Compliance) ให้สอดคล้องกับนโยบายอื่นขององค์กร เช่น ESG นโยบายต่อต้านทุจริต นโยบายบุคลากร นโยบายความปลอดภัย และเป้าหมายเชิงยุทธศาสตร์ขององค์กร

**2. ขอบเขตของนโยบาย**

นโยบายนี้ครอบคลุม:

2.1 คณะกรรมการบริษัท อู่กรุงเทพ จำกัด

2.2 คณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายใน

2.3 ผู้บริหารระดับสูง ประกอบด้วย กรรมการผู้จัดการ รองผู้จัดการ และผู้อำนวยการกอง

2.4 หน่วยงานภายในทั้งหมด

2.5 บริษัทในกลุ่ม / คู่ค้า / ผู้รับเหมาช่วงที่เกี่ยวข้องกับภารกิจหลักขององค์กร

**3. หลักการสำคัญ**

3.1 หลักธรรมาภิบาล (Governance) ➔ **ความโปร่งใส ความรับผิดชอบ**

บริษัทมุ่งมั่นดำเนินงานภายใต้หลักธรรมาภิบาล 5 ประการ ได้แก่ ความโปร่งใส (Transparency) การรับผิดชอบ (Accountability) ความคุ้มค่า (Value for Money) การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย (Stakeholder Engagement) และการยึดมั่นในกฎหมายและจริยธรรม (Integrity & Compliance)

3.2 นโยบายการบริหารความเสี่ยง (Risk Management Policy) ➔ **ป้องกัน-เตือนล่วงหน้า**

3.3.1 การบริหารความเสี่ยง

บริษัทฯ กำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการตัดสินใจเชิงกลยุทธ์ โดยใช้กรอบ COSO ERM 2017 ในการระบุ ประเมิน ตอบสนอง และติดตามความเสี่ยง บูรณาการความเสี่ยงเข้ากับแผนยุทธศาสตร์ แผนปฏิบัติการ และงบประมาณ จัดทำ Risk Portfolio เพื่อมองเห็นภาพรวมของความเสี่ยงองค์กร และใช้ระบบ Early Warning และ Leading Indicators เพื่อเตือนล่วงหน้า

3.3.2 การบริหารความเสี่ยงเชิงรุก

บริษัทฯ มุ่งมั่นดำเนินการบริหารความเสี่ยงเชิงรุก โดยการกำหนดแนวทางที่คาดการณ์ล่วงหน้า เพื่อระบุและจัดการความเสี่ยงก่อนที่จะเกิดปัญหาขึ้นจริง โดยจะพิจารณาแนวโน้มและรูปแบบจากข้อมูลในอดีต เพื่อคาดการณ์ความเสี่ยงที่อาจเกิดขึ้นในอนาคตและวางแผนป้องกันหรือบรรเทาความเสี่ยงเหล่านั้น ซึ่งจะช่วยลดความเสียหายที่อาจเกิดขึ้นได้ดีกว่าการแก้ไขหลังจากเหตุการณ์ผ่านไปแล้ว

3.3 นโยบายการควบคุมภายในและการปฏิบัติตามข้อกำหนด (Internal Control & Compliance Policy) ➔ **ความมั่นคง ปฏิบัติตามกฎหมาย**

3.3.1 พัฒนาระบบควบคุมภายในตามกรอบ COSO 2013

3.3.2 ให้หน่วยงานทุกระดับต้องประเมินประสิทธิผลของการควบคุม (Control Effectiveness)

3.3.3 มีระบบติดตามการปฏิบัติตามกฎหมาย พ.ร.บ.จัดซื้อจัดจ้าง กฎหมายสิ่งแวดล้อม กฎหมายแรงงาน ด้านความปลอดภัย ฯลฯ

3.3.4 มีการตรวจสอบภายใน (Internal Audit) ตามแนวทาง Risk-Based Audit

3.3.5 ระบบควบคุมภายในที่มีประสิทธิภาพ

บริษัทมุ่งมั่นดำเนินการกำหนดระบบที่สร้างความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ได้ โดยอาศัยการดำเนินงานตาม 5 องค์ประกอบหลัก คือ สภาพแวดล้อมการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุม สารสนเทศและการสื่อสาร และการติดตามตรวจสอบ พร้อมกับการมีผู้นำที่ดี การกำหนดโครงสร้างที่ชัดเจน และความร่วมมือจากทุกคนในองค์กร

3.3.6 การปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานสากล

บริษัทมุ่งมั่นดำเนินการปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานสากล โดยการกระบวนการเพื่อให้แน่ใจว่าองค์กรปฏิบัติตามกฎหมาย กฎระเบียบ และมาตรฐานที่กำหนดในแต่ละประเทศ เพื่อหลีกเลี่ยงความเสี่ยงทางกฎหมายและชื่อเสียง เพิ่มความน่าเชื่อถือ และเพิ่มโอกาสทางธุรกิจ ซึ่งครอบคลุมหลายด้าน เช่น กฎหมายแรงงาน ภาษี สิ่งแวดล้อม ความปลอดภัย และการคุ้มครองข้อมูล

**4. แนวทางเผยแพร่นโยบาย (GRC Communication Framework)**

เพื่อให้การเผยแพร่เกิดผลลัพธ์จริงและสามารถรายงานต่อคณะกรรมการได้อย่างมีหลักฐานรองรับ ควรดำเนินการดังนี้

4.1 ช่องทางภายในองค์กร

4.1.1 Intranet และระบบสารสนเทศ: หน้าแรกของระบบต้องปรากฏนโยบาย GRC + ลิงก์ไปยังคู่มือ

4.1.2 E-mail สื่อสารจากกรรมการผู้จัดการ: เป็นทางการ เพื่อแสดงความสำคัญระดับองค์กร

4.1.3 การบรรยายชี้แจง (Kick-off Session): สำหรับหัวหน้าสายงาน ⟶ ถ่ายทอดต่อระดับปฏิบัติ

4.1.4 Infographic และโปสเตอร์: ติดตั้งในพื้นที่สำคัญ เช่น โรงซ่อมอู่เรือ, อาคารบริหาร

4.1.5 e-Learning & Quiz: เพื่อประเมินความเข้าใจและใช้เป็นหลักฐาน SE-AM

4.2 ช่องทางภายนอก

4.2.1 เว็บไซต์องค์กร: เผยแพร่นโยบายในส่วน “ธรรมาภิบาล” และ “การบริหารความเสี่ยง”

4.2.2 หนังสือเวียนถึงผู้รับเหมา/คู่ค้าหลัก: เพื่อยืนยันความคาดหวังในการปฏิบัติตามนโยบาย GRC

4.2.3 การนำเสนอใน MOU / TOR: ระบุพันธกรณีเรื่อง GRC

4.2.4 social media องค์กร: เผยแพร่ในรูปแบบ Infographic และแสดงถึงความโปร่งใส

4.3 กลไกติดตามและรับรองผล

| กลไกติดตาม | รายละเอียด | ข้อกำหนด SE-AM ที่ตอบ |
|---|---|---|
| แบบประเมินความเข้าใจพนักงาน | สำรวจรับรู้และรับรองผล | ใช้ยืนยันระดับ 3 |
| รายงาน Dashboard GRC | เสนอคณะกรรมการทุกไตรมาส | ตอบหมวด 5.1 & 5.2 |
| หลักฐานการอบรม | รายชื่อผู้เข้าร่วม + ภาพถ่าย + เอกสาร | ใช้เป็น evidence ระดับ 3 |
| Communication Log | สรุปช่องทางและผู้รับสาร | ใช้ส่ง สคร. |

**5. แนวทางการนำ GRC ไปปฏิบัติอย่างเป็นรูปธรรม**

| ระยะ | การดำเนินงาน | ผลลัพธ์ที่ได้ | เอกสารหลักฐาน SE-AM |
|---|---|---|---|
| **Phase 1** | จัดตั้งคณะกรรมการ กำหนดบทบาท Risk Owner | มีโครงสร้างชัดเจน | TOR, คำสั่งแต่งตั้ง |
| **Phase 2** | จัดทำ Risk Register + GRC KPI | ความเสี่ยงทั้งหมดถูกผูกกับตัวชี้วัด | Risk Map, KPI Matrix |
| **Phase 3** | สื่อสาร/อบรม/Infographic | พนักงานทุกระดับเข้าใจ | รายงานการอบรม, Quiz |
| **Phase 4** | เริ่มใช้ Dashboard + Audit | มีข้อมูลติดตามรายไตรมาส | Dashboard, Audit Report |
| **Phase 5** | ปรับปรุง/พัฒนาให้คะแนนถึงระดับ 4 | องค์กรขับเคลื่อนเชิงรุก | GRC Improvement Plan |

**6. การกำหนด Risk Appetite ระดับองค์กร**

หลักการสำคัญการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite: RA) จะต้องเชื่อมโยงกับเป้าประสงค์ทางการเงินและไม่ใช่การเงิน สะท้อนความสามารถในการรับความสูญเสีย (Loss Absorption Capacity) คำนึงถึงความคาดหวังของผู้ถือหุ้น ภาครัฐ และผู้มีส่วนได้เสียหลัก และมีการกำหนด Risk Tolerance เป็นช่วงเบี่ยงเบนที่วัดผลได้

| ประเภทความเสี่ยง | Risk Appetite (ยอมรับได้) | Risk Tolerance (ช่วงเบี่ยงเบน) |
|---|---|---|
| **การเงิน** | EBITDA ต้องเป็นบวกทุกปี | ไม่ต่ำกว่า 90% ของเป้าหมาย |
| **การดำเนินงาน** | ไม่เกิดการหยุดชะงักของอู่เรือเกิน 24 ชั่วโมง | ไม่เกิน 2 ครั้ง/ปี |
| **ด้านภาพลักษณ์** | ไม่ให้มีเหตุที่กระทบชื่อเสียงในระดับประเทศ | 0 ครั้ง |
| **ด้านกฎหมาย/จัดซื้อจัดจ้าง** | ไม่ให้เกิดการฟ้องร้อง/ผิด พ.ร.บ.จัดซื้อจัดจ้าง | 0 กรณี |
| **ความปลอดภัย** | อุบัติเหตุ Lost Time Injury Rate ≤ 1 | ไม่เกิน 3 กรณี/ปี |

**7. บทบาทของคณะกรรมการและผู้บริหาร**

| ระดับ | หน้าที่หลัก |
|---|---|
| **คณะกรรมการบริษัท** | **อนุมัตินโยบาย GRC และ Risk Appetite, กำกับระดับสูง** |
| **คณะกรรมการบริหารความเสี่ยงฯ** | **กำหนดกรอบการบริหารความเสี่ยง ติดตามและรายงานรายไตรมาส** |
| **ผู้บริหารระดับสูง** | **นำ RA ไปสู่การปฏิบัติ, ผูก KPI กับการบริหารความเสี่ยง** |
| **ผู้ตรวจสอบภายใน** | **ตรวจติดตามความสอดคล้องของ GRC และรายงานโดยอิสระ** |
| **พนักงานทุกระดับ** | **ระบุและบริหารความเสี่ยงในงานตนเองตาม Risk Ownership** |

**8. การรายงานและการติดตาม**

8.1 รายงาน Risk Dashboard ต่อคณะกรรมการอย่างน้อย ไตรมาสละ 1 ครั้ง

8.2 ใช้ Early Warning Indicator ในระบบดิจิทัลเพื่อแจ้งเหตุล่วงหน้า

8.3 ทบทวน RA และ GRC อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

**9. กลไกสร้างวัฒนธรรมนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน (GRC)**

9.1 จัดให้มี Risk Culture Program

9.2 ผูกระบบ ผลตอบแทน/โบนัส กับการบริหารความเสี่ยง

9.3 กำหนดให้ GRC เป็นส่วนหนึ่งของ Competency Framework

**10. ขั้นตอนทบทวนนโยบาย (Implementation-Ready)**

| ขั้นตอน | รายละเอียด | ผลลัพธ์ |
|---|---|---|
| 1. ตั้งคณะทำงานทบทวน | รวมตัวแทนจากฝ่ายแผนยุทธศาสตร์ กฎหมาย HR ความเสี่ยง และตรวจสอบภายใน | มี TOR และแผนการประชุม |
| 2. วิเคราะห์นโยบายที่เกี่ยวข้อง | ตรวจสอบการซ้ำซ้อน ช่องว่าง และความเชื่อมโยง | Policy Mapping Matrix |
| 3. ปรับปรุงเนื้อหานโยบาย GRC | รวม G, R, C ให้สอดคล้องกับ ESG, Anti-Corruption, Digital Governance | Draft Policy Version ใหม่ |
| 4. เสนอคณะกรรมการอนุมัติ | ผ่านกรรมการบริหารความเสี่ยง และบอร์ด | มติอนุมัติใช้ |
| 5. ประกาศใช้ & สื่อสาร | ใช้ช่องทางภายใน + คู่ค้า + เว็บไซต์ | Policy Roll-out Plan |

**11. Policy Mapping Matrix (แผนผังการเชื่อมโยงนโยบาย)**

| นโยบายหลัก | นโยบายที่เกี่ยวข้อง | ความสอดคล้อง | แนวทางการบูรณาการ |
|---|---|---|---|
| GRC | ESG ต่อต้านทุจริต HR | สร้างเสถียรภาพองค์กร | ผสานตัวชี้วัด GRC ในทุกนโยบาย |
| ESG | ความปลอดภัย, สิ่งแวดล้อม | ลดความเสี่ยงสิ่งแวดล้อม | บูรณาการ RA ด้าน ESG |
| ต่อต้านทุจริต | GRC & Compliance | Zero Tolerance | ปรับปรุงกระบวนการควบคุม |

**12. แบบประเมินผลกระทบนโยบาย (Policy Impact Assessment)**

**12.1 วัตถุประสงค์**

เพื่อประเมินผลของนโยบายแต่ละฉบับต่อองค์กรในเชิงกลยุทธ์ การเงิน ความเสี่ยง และความยั่งยืน

**12.2 แบบฟอร์ม**

| ประเด็นประเมิน | คะแนน (1-5) | หมายเหตุ |
|---|---|---|
| ความสอดคล้องกับวิสัยทัศน์องค์กร | | |
| ผลกระทบด้านความเสี่ยง | | |
| ผลกระทบเชิงบวกด้าน ESG | | |
| ความจำเป็นในการปรับปรุง | | |

**13. การทบทวนโยบายกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) เพื่อให้เหมาะสมกับนโยบายอื่นๆ ที่เกี่ยวข้องขององค์กร**

13.1 บูรณาการนโยบายทั้งหมดของบริษัท รวมถึง ESG, HR, Anti-Corruption, คุณภาพ ความปลอดภัย สิ่งแวดล้อม และเทคโนโลยีทางเรือ

13.2 เพิ่มเกณฑ์ควบคุมเชิงรุก (Proactive Control) และระบบการเตือนล่วงหน้าความเสี่ยง (Early Warning System)

13.3 จัดทำตัวชี้วัดระดับองค์กร (Enterprise Risk Indicators) ที่ผูกกับเป้าหมายเชิงยุทธศาสตร์ของรัฐวิสาหกิจด้านความมั่นคงทางทะเล

13.4 กำหนดให้มีการตรวจประเมินตนเอง (Self-Assessment) และ External Audit เพื่อยืนยันประสิทธิผล

13.5 ยกระดับให้ GRC เป็นเครื่องมือขับเคลื่อนนวัตกรรมองค์กร ไม่ใช่เพียงการควบคุม

**14. การปรับปรุงนโยบาย GRC ให้สอดคล้องกับบริบทของรัฐวิสาหกิจและมาตรฐานสากลที่เปลี่ยนแปลงไป**

14.1 ปรับแนวทางกำกับดูแลให้สอดคล้องกับเกณฑ์รัฐวิสาหกิจใหม่ภายใต้คณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

14.2 บูรณาการกรอบ COSO 2017, ISO 31000:2018 และหลักธรรมาภิบาล OECD เพื่อยกระดับมาตรฐาน

14.3 เพิ่มแนวทาง ESG และการบริหารความยั่งยืนตาม SDGs และ Global Reporting Initiative (GRI)

14.4 กำหนดให้มีการประเมินความเสี่ยงเชิงกลยุทธ์ (Strategic & Emerging Risks) ครอบคลุมภัยคุกคามสมัยใหม่ เช่น Cybersecurity, Supply Chain, Geopolitical Risks

14.5 ปรับปรุงระบบควบคุมภายในให้รองรับ Digital Transformation และการใช้ AI/Automation ในการกำกับดูแล

14.6 นำนโยบาย Zero Tolerance และ Integrity Pact มาบังคับใช้เข้มงวด เพื่อสร้างความโปร่งใสและความเชื่อมั่นต่อสาธารณะ

**15. ส่วนการเสริมสร้างกลยุทธ์ (Strategic Enhancement Section)**

15.1 ความเสี่ยงด้านเทคโนโลยีและความมั่นคงไซเบอร์ (Cyber & Digital Risk)

15.1.1 การจัดทำ Cyber Governance Framework เพื่อปกป้องข้อมูลและระบบควบคุมเรือ

15.1.2 บังคับใช้ Data Protection, AI Governance และระบบเตือนภัยไซเบอร์แบบเรียลไทม์

15.1.3 ประเมิน Cyber Maturity ตามมาตรฐาน NIST และ ISO/IEC 27001

15.2 ความเสี่ยงจากการเปลี่ยนแปลงด้านสิ่งแวดล้อมและความมั่นคงทางทะเล (Climate & Maritime Security Risk)

15.2.1 เพิ่มมาตรการ ESG และ Climate Risk เข้าใน Risk Appetite ขององค์กร

15.2.2 รองรับกฎหมาย IMO, Carbon Tax และผลกระทบต่ออุตสาหกรรมเรือพาณิชย์และป้องกันประเทศ

15.2.3 กำหนด Maritime Security Protocol ในการบริหารความเสี่ยงเชิงภูมิรัฐศาสตร์

15.3 การสร้างมูลค่าจาก GRC (Value Creation through Governance)

15.3.1 ใช้ GRC เป็นเครื่องมือสนับสนุนนวัตกรรมและการลงทุนเชิงกลยุทธ์

15.3.2 สร้างกลไกให้ GRC ไม่ใช่เพียง Compliance แต่เป็นตัวขับเคลื่อนการเติบโตขององค์กร

15.3.3 ผูก GRC กับ KPI เชิงกลยุทธ์และ Performance Excellence ตาม SE-AM และ PMQA

**16. การอ้างอิงมติและบทเฉพาะกาล**

16.1 มติที่เกี่ยวข้อง

16.1.1 มติคณะรัฐมนตรีว่าด้วยการกำกับดูแลรัฐวิสาหกิจด้านธรรมาภิบาลและความโปร่งใส

16.1.2 มติคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) เกี่ยวกับการบริหารความเสี่ยงเชิงยุทธศาสตร์

16.1.3 แนวทางของกองทัพเรือในการกำกับดูแลความมั่นคงทางทะเลและอุตสาหกรรมป้องกันประเทศ

16.2 บทเฉพาะกาล (Transition Phase)

16.2.1 การบังคับใช้ของนโยบายฉบับนี้จะดำเนินการเป็นระยะ (Phase 1 – 3) เพื่อให้หน่วยงานสามารถปรับระบบบริหารจัดการภายในให้สอดคล้อง

16.2.2 ในช่วงเปลี่ยนผ่าน อนุญาตให้ใช้คู่ขนานระหว่างนโยบายเดิมและนโยบายฉบับปรับปรุง โดยมีคณะทำงานกำกับดูแลการเปลี่ยนผ่านอย่างใกล้ชิด

16.2.3 ภายใน 12 เดือนหลังประกาศใช้ จะต้องมีรายงานผลการนำไปปฏิบัติต่อคณะกรรมการ พร้อมข้อเสนอเพื่อปรับปรุง

**7. แถลงเจตนารมณ์จากกรรมการผู้จัดการ**

บริษัท อู่กรุงเทพ จำกัด มีความมุ่งมั่นที่จะดำเนินงานด้วยหลักธรรมาภิบาล โปร่งใส ตรวจสอบได้ และบริหารความเสี่ยงอย่างรอบด้านตามมาตรฐานสากล เพื่อเสริมสร้างสมรรถนะองค์กรให้เป็นกลไกสำคัญของประเทศด้านอุตสาหกรรมซ่อมสร้างเรือและการป้องกันประเทศ พร้อมทั้งยึดมั่นในการควบคุมภายในอย่างเข้มแข็งเพื่อสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย และการเติบโตอย่างยั่งยืนในระยะยาว

**ลงชื่อ.....**

(ประธานกรรมการบริษัท อู่กรุงเทพ จำกัด

วันที่ ..... เดือน ..... พ.ศ. .....