اسمنت اليمامة
YAMAMA CEMENT

سياسة أمن المعلومات

الكود:	ISP613-26
الإصدار:	1.0
تاريخ الإصدار:	March 30, 2017
إعداد:	رضوان أحمد
مستوى السرية:	عام

تاريخ التغيير

وصف التغيير	مراجعة	إعداد	الإصدار	التاريخ
التفاصيل الكاملة المحددة عن سياسة أمن المعلومات	جعفر العريفي، عبدالله الفرهود	رضوان أحمد	1.0	2017-03-30
تمت مراجعة السياسة	لجين نتو	رضوان أحمد	1.0	2019-12-01

جدول المحتويات

1. الغرض، النطاق والمستخدمين

"المعلومات" تعتبر أحد الأصول ويجب أن تكون محمية بشكل مناسب. يقوم "أمن المعلومات" بحماية الأصول من مجموعة واسعة من التهديدات لضمان استمرار العمليات التجارية ، وتوفير القيمة لأصحاب المصلحة ، وتحقيق أقصى عائد على الاستثمارات.

يتم تحقيق أمن المعلومات من خلال تنفيذ مجموعات مناسبة من الضوابط الإدارية والمادية والفنية ، وهي السياسات والممارسات والإجراءات والهياكل التنظيمية والتكنولوجيا والبرمجيات. يشار إلى اسمنت اليمامة بـ"المنظمة" أو "اسمنت اليمامة" في هذه الوثيقة ، لإنشاء ضوابط أمنية لتحقيق الأهداف الخاصة بأمن المعلومات.

الهدف من السياسة العالية الأهمية هذه هو تحديد الغرض والتوجه والمبادئ والقواعد الأساسية لإدارة أمن المعلومات.

يتم تطبيق هذه السياسة على نظام إدارة أمن المعلومات بالكامل.**(ISMS)**

مستخدمو هذا المستند هم جميعًا موظفين في اسمنت اليمامة ، بالإضافة إلى الأطراف الخارجية ذات الصلة.

2. المستندات المرجعية

- المعيار **ISO / IEC 27001** ، الفقرات 5.2 و 5.3
- تقييم المخاطر ومنهجية معالجة المخاطر "**Risk Assessment & Risk Treatment Methodology**"
- بيان قابلية التطبيق

3. مصطلحات أمن المعلومات الأساسية

السرية "Confidentiality " - خصائص المعلومات التي تكون متاحة فقط للأشخاص المصرح لهم أو الأنظمة المصرح لها.

النزاهة "Integrity" - هي خصائص المعلومات التي يتم تغييرها فقط من قبل أشخاص أو أنظمة بطريقة مسموح بها.

التوفر "Availability" - خاصية المعلومات التي يمكن الوصول إليها من قبل الأشخاص المخولين عند الحاجة.

أمن المعلومات "Information Security" - الحفاظ على سرية ونزاهة وتوافر المعلومات.

نظام إدارة أمن المعلومات "ISMS" - جزء من عمليات الإدارة الشاملة التي تهتم بتخطيط ، وتنفيذ ، وصيانة ، ومراجعة ، وتحسين أمن المعلومات.

4. إدارة أمن المعلومات

4.1 الأهداف والقياسات

تتمثل الأهداف العامة لنظام إدارة أمن المعلومات فيما يلي: إنشاء صورة سوقية أفضل "**Better Market Image**" والحد من الأضرار الناجمة عن الحوادث المحتملة ؛ الأهداف تتماشى مع أهداف الشركة التجارية واستراتيجيتها وخطط أعمالها. مدير أمن المعلومات هو المسؤول عن مراجعة هذه الأهداف العامة لنظام إدارة أمن المعلومات وإعداد أخرى جديدة.

يتم اقتراح أهداف ضوابط الأمن الفردية أو مجموعات من عناصر التحكم والموافقة عليها في بيان القابلية للتطبيق.

يجب مراجعة جميع الأهداف مرة واحدة في السنة على الأقل.

سوف تقيس اسمنت اليمامة تحقيق جميع الأهداف. مدير أمن المعلومات هو المسؤول عن تحديد طريقة قياس إنجاز الأهداف - يتم إجراء القياس مرة واحدة على الأقل في السنة ويقوم مدير أمن المعلومات / المدقق الداخلي بتحليل نتائج القياس وتقييمها وتقديم تقرير عنها إلى الإدارة العليا كمدخلات "**Input**" من مراجعة الإدارة.

4.2. ضوابط أمن المعلومات

يتم تحديد عملية اختيار الضوابط (**Safeguards**) في منهجية تقييم المخاطر ومعالجة المخاطر.

يتم سرد عناصر التحكم المحددة وحالة التنفيذ الخاصة بها في بيان قابلية التطبيق.

4.3. المسؤوليات

تتمثل مسؤوليات نظام إدارة أمن المعلومات فيما يلي:

اسم الوظيفة/اسم المجموعة	المسؤولية
الإدارة العليا / منتدى أمن المعلومات	مسؤول عن ضمان إنشاء نظام إدارة أمن المعلومات ويتوافق مع متطلبات **ISO 27001: 2013.** والتأكد من مراجعة نظام إدارة أمن المعلومات لملاءمته وكفاءته وفعاليته
مدير أمن المعلومات / المدقق الداخلي	مسؤول عن تقديم التقارير عن أداء نظام إدارة أمن المعلومات إلى الإدارة العليا.
الموارد البشرية / مدير امن المعلومات	مسؤول عن تطوير وتنفيذ خطة التوعية التدريبية "Training Awareness" لموظفي أسمنت اليمامة.
مالك الأصل	مسؤول عن الحفاظ على سرية ونزاهة وتوافر الأصول.
مدير أمن المعلومات	مسؤول عن ضمان توافر سياسة الأمن وتوصيلها إلى جميع موظفي اسمنت اليمامة ، وكذلك الأطراف الخارجية المعنية يجب أن تكون على دراية بهذه السياسة.

4.4. معرفة السياسة

يجب على مدير أمن المعلومات التأكد من أن جميع موظفي إسمنت اليمامة، وكذلك الأطراف الخارجية المعنية ، على دراية بهذه السياسة.

5. مراجعة سياسة أمن المعلومات

منتدى أمن المعلومات هو المسؤول عن مراجعة سياسة أمن المعلومات في فترات زمنية محددة. يجب مراعاة النقاط التالية عند مراجعة السياسة وتحديثها:

- التغييرات في بيئة الشركة أو ظروف العمل أو توفر الموارد أو الشروط التعاقدية أو التنظيمية أو القانونية أو البيئة التقنية
- ردود فعل "**Feedback**" من أطراف مختلفة مثل المراجعين الخارجيين والداخليين والبائعين الخارجيين والمستخدمين
- نتائج المراجعات المستقلة
- حالة الإجراءات التصحيحية
- نتائج مراجعات الإدارة السابقة
- الامتثال لسياسة أمن المعلومات
- حوادث أمن المعلومات التي تم الإبلاغ عنها
- التوصيات المقدمة من السلطات المختصة

تتمثل مسؤوليات التنفيذ والإدارة في منتدى أمن المعلومات.

5.1. الاستثناءات

يجب أن توافق الإدارة مسبقًا على أي استثناء من هذه السياسة أو أي سياسات أخرى في إطار تنفيذ نظام إدارة أمن المعلومات.

5.2. عدم الامتثال

قد يخضع أي موظف يتبين أنه انتهك هذه السياسة أو أي سياسات أخرى في إطار نظام إدارة أمن المعلومات لإجراءات تأديبية وفقًا لسياسة الشركة.

6. التزام الإدارة

تلتزم شركة اسمنت اليمامة ببيئة مراقبة شاملة تشمل السياسات والعمليات وأنشطة التحكم للتأكد من أن أنظمة المعلومات في الشركة محمية بشكل ملائم. يتم تطوير خطط الأعمال الاستراتيجية طويلة الأجل وقصيرة الأجل وإبلاغها لتوضيح رؤية المنظمة لأصحاب المصلحة فيها.

ولتحقيق ذلك ، يتم إجراء تقييم للمخاطر سنويًا لتحديد المخاطر ، والتنفيذ اللاحق للضوابط لتخفيف المخاطر أو إدارتها بشكل مناسب. تلتزم إدارة أسمنت اليمامة بتوفير الموارد والوقت والموافقات لتنفيذ أهداف أمن المعلومات ، مع السعي إلى التحسين المستمر.

من أجل الحفاظ على أمن المعلومات وإشراكها في ممارساتها وتقليل تعرضها للمخاطر من خلال تطبيق الضوابط في بيئة الشركة ، بالتالي فإن سياسة إسمنت اليمامة هي لضمان:

- إنشاء نظام إدارة أمن المعلومات بناءً على متطلبات معيار **ISO IEC 27001:2013**
- تحديد مخاطر أمن المعلومات وتنفيذها وإدارتها من أجل الحفاظ على سرية ونزاهة وتوافر نظم المعلومات والمعلومات.
- تحديد وإدارة احتياجات أمن المعلومات وتوقعات عملاء المنظمة والمساهمين والشركاء.
- عندما يتم الاستعانة بمصادر خارجية لخدمات المنظمة ، سيتم التحكم في أمن المعلومات من خلال العقود وتحديد متطلبات الأمن واتفاقيات مستوى الخدمة وعمليات التدقيق.

- الإبلاغ عن جميع حوادث عدم المطابقة "**non-conformances**" وأمن المعلومات والتحقيق فيها من قبل مدير أمن المعلومات وسيتم اتخاذ الإجراء المناسب في الوقت المناسب.
- تخطيط خطط استمرارية الأعمال "**Business Continuity Plans**" للأنشطة الحيوية المهمة وحمايتها واختبارها.
- مراجعة فعالية وكفاءة نظام إدارة أمن المعلومات من خلال التدقيق الداخلي / الخارجي ومراجعات الإدارة.
- تحديد متطلبات تدريب وتطوير أمن المعلومات ومعالجتها لفرق أمن المعلومات.

7. الدعم لتنفيذ نظام إدارة أمن المعلومات

بموجب هذا ، تعلن الإدارة العليا أن تنفيذ نظام إدارة أمن المعلومات والتحسين المستمر سيتم دعمه بموارد كافية من أجل تحقيق جميع الأهداف المحددة في هذه السياسة ، وكذلك تلبية جميع المتطلبات المحددة.

8. صلاحية وإدارة الوثيقة

هذه الوثيقة صالحة اعتبارًا من **30** مارس 2017.

مالك هذا المستند هو مدير أمن المعلومات ، الذي يجب أن يدقق ، وإذا لزم الأمر ، أن يحدث المستند مرة واحدة على الأقل كل عام.

عند تقييم فعالية وكفاءة هذا المستند ، يجب مراعاة المعايير التالية:

- عدد الموظفين والأطراف الخارجية الذين لهم دور في نظام إدارة أمن المعلومات ، لكنهم ليسوا على دراية بهذه الوثيقة
- عدم امتثال نظام إدارة أمن المعلومات للقوانين واللوائح والالتزامات التعاقدية وغيرها من الوثائق الداخلية للمنظمة
- عدم فعالية تنفيذ نظام إدارة أمن المعلومات وصيانتها
- مسؤوليات غير واضحة لتنفيذ نظام إدارة أمن المعلومات

تمت الموافقة عليه من قبل:
السيد/ باسم الحازمي
مدير تقنية المعلومات بشركة إسمنت اليمامة

_____