Cyber Security Policy Statement

Reference: ST-IT,I&C-DOC-001

Cyber security is an important concern for all STOMO operated and maintained assets. Internet-connected means of communication are omnipresent in today's modern technological world. One of the security challenges been faced is the proliferation of cyber technology and possible associated risks and hence it is vital to have an institutionally as well as physically coherent and coordinated set of tools to prevent unauthorized access to our critical infrastructure. STOMO's Cyber security policy defines a strategic framework aligned with the Asset Owners and external Stakeholders with the intent to monitor and control internal and external access to its IT and Industrial Control networked systems and the information they contain.

STOMO's Cyber security policy is based on a proactive approach; accordingly, it seeks to ensure that threats are detected early, analysed thoroughly and that active measures are put into place. It is STOMO management's goal to work with the Owners and Stakeholders to safeguard the Assets from known Cyber threats by exercising proficiencies of PREVENT, DETECT & RESPOND utilizing our PEOPLE, PROCESS & TECHNOLOGY to achieve CONFIDENTIALITY, INTEGRITY & AVAILABILITY of all critical IT and Industrial Control systems at all times. Based on a risk review approach and in coordination with the Owners appropriate technical tools, systems and processes will be established and utilized to achieve these goals.

STOMO commits to comply with local legal obligations in support of the Owners meeting the expectations to satisfy the stakeholders. Clearer communication shall be delivered among all STOMO employees creating a cyber security culture, enabling everyone to know their responsibilities and what needs to be done if an incident occurred or is suspected. This shall be delivered by means of awareness campaigns to increase the staff knowledge of competence in relation to Cyber security.

يعتبر الأمن السيبراني (Cyber Security) بالغ الأهمية لشركة ستومو والأجهزة المتعلقة بها. في الوقت الراهن أصبحت الأجهزة المتصلة بالأنترنت منتشرة وبكثرة مما يجعله تحديا كبير للأمن السيبراني. لذالك لمواجهة هذا الخطر يجب أن تكون للشركة مجموعة متكاملة من الأدوات لمنع الوصول الغير المصرح له لأي من البنية التحتية الحيوية بالشركة. من أجل ذالك وضعت ستومو مجموعة من القوانين والأطر لمراقبة والتحكم بكل البيانات المتدفقة خارجيا و داخليا لأجهزة نظم والمعلومات و شبكة تشغيل المحطة والأجهزة التابعة لها.

وتقوم سياسة الأمن السيبراني لستومو على نهج إستباقي , وذلك النهج يقوم بالكشف عن التهديدات في وقت مبكر قبل وقوعها و تحليلها تحليلا دقيقا ووضع كل التدابير الفعالة بمكانها. هذا هو هدف وسياسة الشركة بالعمل مع الملاك وأصحاب المصلحة لحماية الممتلكات من المخاطر السيبرانية من خلال تطبيق بعض من مهارات الحماية, الكشف المبكر, التجاوب السريع باستخدام القدرات البشرية و التكنولوجية لتحقيق السرية, النزاهة, و توافر جميع أنظمة المعلومات الحساسة و أنظمة التحكم بالشركة في كل وقت. بمساعدة من المالك يجب علينا استثمار أفضل الأدوات و الطرق لتحقيق أهدافنا. استنادا الى نهج مراجعة المخاطر وبالتنسيق مع الملاك وباستخدام الأدوات التقنية، والأنظمة و الطرق الملائمة لتحقيق هذه الأهداف.

ونحن نلزم أنفسنا بالأمتثال بالقوانين المحلية بمساعدة الملاك لتحقيق التوقعات لارضاء أصحاب المصلحة لدينا. إن وضوح طرق التواصل بين جميع موظفي الشركة تصنع ثقافة الأمن السيبراني و تسمح لكل موظف و موظفة بمعرفة مسؤولياته وما هي الأجراءات التي يجب اتباعها عند وقوع حادثة أو الاشتباه بوقوعها, وهذه سيتم تناولها من خلال الحملات التوعوية لزيادة المعرفة و الكفاءة بما يتعلق بالأمن السيبراني.

Signed: _____

Luc Dietvorst (CEO)

Date: 01 January 2018