

Data Security & Information Policy

Environmental Horizons Co. (EH) regards data, information, and digital assets as among its most critical institutional assets requiring continuous protection, recognizing that information confidentiality, integrity, availability, and privacy are fundamental pillars of business continuity, the protection of stakeholders' interests, the enhancement of client trust, and the preservation of the Company's reputation.

Environmental Horizons Co. is committed to protecting all its data, information, and digital assets against unauthorized access, disclosure, modification, destruction, loss, or misuse, through the implementation of appropriate information security and cybersecurity controls and procedures that are aligned with applicable regulatory and contractual requirements and recognized best practices.

All EH-related data and information shall be stored exclusively in Company-approved systems, including ERP systems, authorized cloud platforms, and approved servers and databases. The storage, transfer, or sharing of Company data via personal devices, storage media, applications, or unapproved systems is strictly prohibited.

Information shall be classified in accordance with the Company's approved classification levels - Public, Internal, Restricted, and Confidential - with appropriate protection controls applied to each level, encompassing access control, encryption, storage, transfer, and secure disposal of information. Access to information shall be granted in accordance with the Need-to-Know principle and the Least Privilege Principle, limited to what is necessary for the performance of job responsibilities.

All employees, contractors, consultants, service providers, and third parties authorized to access Company information are required to maintain its confidentiality, protect it, and use it solely for authorized purposes, and to immediately report any actual or suspected security incident, threat, or vulnerability to the QHSE Department and the Digitization Department in accordance with approved procedures.

Environmental Horizons Co. maintains a zero-tolerance approach towards any negligence, misuse, or unauthorized disclosure of information. The Company guarantees full protection to anyone who reports a security incident or violation in good faith, and expressly prohibits any form of retaliation, discrimination, or adverse impact as a result of such reporting.

The Company is committed to developing and continuously improving its cybersecurity and information security capabilities through the implementation of access control measures, identity and privilege management, backup and recovery, vulnerability management, system monitoring, ongoing awareness and training, and business continuity and disaster recovery readiness testing, thereby ensuring the mitigation of cyber risks and the preservation of operational continuity. This policy reflects Environmental Horizons Co.'s commitment to compliance with the regulations, rules, and instructions issued by relevant regulatory authorities, including the requirements of the National Cybersecurity Authority (NCA), applicable client contractual requirements where relevant, the international standard ISO/IEC 27001, and recognized best practices in the fields of information security and cybersecurity.

This policy shall be reviewed periodically to ensure its continued alignment with the Company's strategy, the nature of its business, applicable legal, regulatory, and contractual requirements, and recognized best practices.

سياسة أمن البيانات والمعلومات

تعتبر شركة آفاق البيئة البيانات والمعلومات والأصول الرقمية من أهم أصولها المؤسسية التي تستوجب الحماية المستمرة، إذ تُقرّ الشركة بأن سرية المعلومات وسلامتها وتوافرها وخصائصها تمثل ركائز أساسية لاستمرارية الأعمال، وحماية مصالح أصحاب المصلحة، وتعزيز ثقة العملاء، والمحافظة على سمعة الشركة.

تلتزم شركة آفاق البيئة بحماية جميع بياناتها ومعلوماتها وأصولها الرقمية من الوصول غير المصرح به أو الإفصاح أو التعديل أو الإلحاق أو الفقدان أو سوء الاستخدام، وذلك من خلال تطبيق ضوابط وإجراءات أمن المعلومات والأمن السيبراني المناسبة والمتوافقة مع المتطلبات النظامية والتعاقدية وأفضل الممارسات المعتمدة.

تُحفظ جميع البيانات والمعلومات المتعلقة بشركة آفاق البيئة حصراً في الأنظمة المعتمدة من الشركة، بما في ذلك أنظمة تخطيط موارد المؤسسة، والمنصات السحابية المعتمدة، والخوادم وقواعد البيانات المصرح بها. ويُمنع منعاً باتاً تخزين أو نقل أو مشاركة بيانات الشركة عبر أجهزة شخصية أو وسائط تخزين أو تطبيقات أو أنظمة غير معتمدة.

تُصنّف المعلومات وفق مستويات التصنيف المعتمدة بالشركة (عام، داخلي، مقيد، سري)، وتُطبّق ضوابط الحماية المناسبة لكل مستوى، بما يشمل التحكم في الوصول والتشفير والحفظ والنقل والإلحاق الآمن للمعلومات. ويُمنح الوصول إلى المعلومات وفق مبدأ الحاجة إلى المعرفة وأمل الصلاحيات اللازمة لأداء المهام الوظيفية.

يلتزم جميع الموظفين والمقاولين والاستشاريين ومزودي الخدمات والأطراف الثالثة المصرح لهم بالوصول إلى معلومات الشركة بالمحافظة على سريتها وحمايتها واستخدامها للأغراض المصرح بها فقط، والإبلاغ الفوري عن أي حادثة أو تهديد أو ضعف أمني فعلي أو مشتبه به إلى إدارة الجودة والصحة والسلامة والبيئة وقسم الرقمنة وفق الإجراءات المعتمدة.

تتبنى شركة آفاق البيئة مبدأ عدم التسامح مع أي إهمال أو إساءة استخدام أو إفشاء غير مصرح به للمعلومات، كما تكفل الحماية الكاملة لكل من يُبلغ بحسن نية عن أي حادثة أو مخالفة أمنية، وتحظر أي شكل من أشكال الانتقام أو التمييز أو التأثير السلبي نتيجة هذا الإبلاغ.

وتلتزم الشركة بتطوير وتحسين قدراتها في مجال الأمن السيبراني وأمن المعلومات من خلال تطبيق ضوابط التحكم في الوصول، وإدارة الهوية والصلاحيات، والنسخ الاحتياطي والاستعادة، وإدارة الثغرات الأمنية، ومراقبة الأنظمة، والتوعية والتدريب المستمر، واختبار جاهزية استمرارية الأعمال والتعافي من الكوارث، بما يضمن الحد من المخاطر السيبرانية والحفاظ على استمرارية العمليات.

تعكس هذه السياسة التزام شركة آفاق البيئة بالامتثال للأنظمة واللوائح والتعليمات الصادرة عن الجهات التنظيمية ذات العلاقة، بما في ذلك متطلبات الهيئة الوطنية للأمن السيبراني، والمتطلبات التعاقدية الخاصة بالعملاء عند الاقتضاء، والمعيار الدولي ISO/IEC 27001، وأفضل الممارسات المعتمدة في مجال أمن المعلومات والأمن السيبراني.

تُراجَع هذه السياسة بصورة دورية لضمان استمرار ملاءمتها لاستراتيجية الشركة وطبيعة أعمالها والمتطلبات القانونية والتنظيمية والتعاقدية وأفضل الممارسات المعتمدة.

Eng. Amin Mohammed Ali
Chief Executive Officer

م. أمين محمد علي
الرئيس التنفيذي

