Ref: POL-ISD-029
Date: 11 NOV 25
Version: 2.1
Classification: Public

Transguard Group LLC - Information Security, Privacy and Business Continuity Policy Statement

Transguard Group LLC ("Transguard") is committed to maintaining the appropriate protection of business information, business continuity, and information processing systems, essential to the continuation of its business, its competitive position in the global and local market, and to the success and achievement of its mission and vision.

Transguard has established and implemented an Information Security Management System ("ISMS"), Privacy Information Management System ("PIMS"), and Business Continuity Management System ("BCMS") in line with international standards – ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO 22301:2019 – ensuring robust information security and privacy assurance to support Transguard vision and mission.

Transguard is committed to building on the success of ISMS, improving its security, privacy, and business continuity position, and protecting Transguard from threats, deliberate or accidental, that could negatively impact its operations, reputation, business continuity, and/or the privacy of its customers and employees.

Transguard is also committed to the following:

- Develop, implement, monitor, audit, and continually improve information security, privacy, and business continuity controls in compliance with ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 22301:2019 and national regulations.
- Establish responsibility and accountability for information security, privacy and business continuity within Transguard to protect information processing facilities and personal data from cyber threats, breaches, and/or unauthorised access.
- Ensure compliance with the information security, privacy, and business continuity policies, procedures, and controls.
- Maintain confidentiality, integrity, and availability of information and/or personal data to meet business needs, client requirements, continuity objectives, and privacy obligations.
- Reduce Transguard's exposure to risks from internal and/or external threats, protect its assets, information, systems, infrastructure, critical operations, and/or reputation.
- Foster and improve the level of information security, privacy, and business continuity awareness, knowledge, and skills across all employees.
- Systematically assess, monitor, and manage information security, privacy, and business continuity risks through a structured risk management framework.
- Proactively detect and respond to information security, privacy, and business continuity incidents, monitor for security breaches, and enforce third-party compliance with information security and privacy requirements.
- Continuously monitor and improve ISMS, PIMS and BCMS to meet evolving business and regulatory requirements.

Transguard has appointed the Chief Financial and Support Services Officer to establish, monitor, and improve ISMS, PIMS and BCMS to ensure compliance with information security, privacy, and business continuity policies throughout the organisation, ensuring alignment with internal policies and regulatory requirements. To maintain impartial oversight and strategic governance, escalate and report all information security, privacy, and business continuity incidents, including personal data breaches, cyber threats, and operational disruption directly to the Chief Executive Officer.

All managers are directly accountable for ensuring that information security, privacy, and business continuity policies are enforced within their respective areas. Every employee is responsible for complying with the controls and procedures outlined in the information security and privacy programme for their business unit. All employees, contractors, and vendors with access to Transguard's information assets and personal data are responsible to adhere to the protections and procedures outlined in this policy statement.

Transguard's Leadership Team and senior management of each business unit are committed to ensuring the implementation of this policy statement, with regular reviews to ensure its continued relevance, compliance, implementation and effectiveness.

We entrust the Information Security, Privacy, and Business Continuity policy to all our employees, encouraging them to support and demonstrate dedication and professionalism in making this policy effective while performing their duties on behalf of Transguard. This policy will be reviewed annually as part of the overall management review conducted by the Transguard Information Security, Privacy and Business Continuity Head. This Policy will also be reviewed in response to significant changes in Transguard environment that required update in the policy statement.

Rabie Atieh
Chief Executive Officer

Transguard Group LLC
P.O. Box: 22630 - Transguard Group Headquarters
Airport Freezone, Dubai, United Arab Emirates
T. +971 4 703 0500 F. +971 4 299 5664
E-mail : info@transguardgroup.com
Website : www.transguardgroup.com
TRN: 100225443900003

ترانسجارد جروب ش.ذ.م.م
ص.ب ٢٢٦٣٠ ترانسجارد جروب المقر الرئيسي
المنطقة الحرة بمطار دبي – الإمارات العربية المتحدة
هاتف: ٠٥٠٠ ٧٠٣ ٤ ٩٧١+ – فاكس ٥٦٦٤ ٢٩٩ ٤ ٩٧١+
البريد الإلكتروني: info@transguardgroup.com
الموقع الإلكتروني: www.transguardgroup.com
ترن: ١٠٠٢٢٥٤٤٣٩٠٠٠٠٣