Fortifying the Digital Frontier: Cyber Resilience & Data Security

Data privacy and cybersecurity are critical to REC's operations. REC Has created CISO division strategically as it manage confidential financial and project-related data, protecting this information and ensuring compliance with privacy regulations are paramount. This commitment ensures business continuity and maintains the trust of stakeholders.

1. Robust Governance & ISO Certification

REC has implemented stringent cybersecurity measures and a robust governance structure to mitigate risks across all business processes:

- *ISO 27001:2013 Adherence:* REC successfully completed Surveillance Audit 2 for the internationally recognized ISO 27001:2013 framework, demonstrating our commitment to global security standards.
- *Policy Evolution:* On January 1, 2025, REC comprehensively reviewed and updated its Information Security Management System (ISMS). This includes critical protocols for Backup & Recovery, Data Center (DC) & Disaster Recovery (DR) Plans, and the Security Manual.
- *Management Directives: Our* Data Privacy Policy outlines clear directives on security controls, ensuring that cyber threat risks are addressed across every department.

2. Technical Resilience & Monitoring

We maintain a high-readiness posture to secure our IT landscape in the event of a cyberattack:

- *Continuous Monitoring:* We employ real-time monitoring of our IT systems to promptly identify and respond to security issues.
- *Comprehensive Framework:* Our cybersecurity strategy combines advanced technical measures with procedural compliance to ensure rapid recovery and data integrity.
- *Regulatory Alignment:* We regularly update our privacy frameworks to remain compliant with evolving national and international data regulations.

3. Human Firewall: Awareness & Vigilance

Recognizing that security is a collective responsibility, REC's **CISO Division** spearheaded several high-impact awareness initiatives in FY 2024-25:

- *Targeted Training:* Hosted four specialized cybersecurity sessions led by internal and external experts (July, November, December 2024, and January 2025) for all permanent and non-permanent staff.
- *Phishing Simulations:* Conducted regular exercises to test and improve employee vigilance against sophisticated phishing attempts.
- *Cyber Security Awareness Month (Oct 2024):* Observed a dedicated month featuring expert-led sessions, weekly thematic emails, office-wide posters/standees, and interactive quizzes to embed "Cyber Hygiene" into the corporate culture.
- *Direct Communication:* Distributed SMS alerts and deployed "Dos and Don'ts" wallpapers on all corporate systems to keep security best practices top-of-mind.

Our Commitment: By combining technical excellence with a culture of vigilance, REC Limited ensures that our digital infrastructure remains as resilient as the physical infrastructure we finance.