



# VITROX CORPORATION BERHAD

Registration No.: 200401011463 (649966-K)

746, Persiaran Cassia Selatan 3, Taman Perindustrian Batu Kawan

14110 Bandar Cassia, Pulau Pinang, Malaysia

Tel: (+604) 545 9988 Fax: (+604) 545 9987

www.vitrox.com

## Information Security Management Policy Dasar Pengurusan Keselamatan Maklumat

### Information Security Policy Implementation Pelaksanaan Dasar Keselamatan Maklumat

The number of information security breaches has been growing exponentially over the past decade. Many incidents have shown that information security has become a financially material issue which has to be managed diligently to protect corporate value. ViTrox's Information Security Policy is designed to safeguard confidentiality, integrity and availability of all information assets to increase customer confidence, raise the company's competitiveness and prevent operational disruptions. ViTrox strives to achieve zero (0) cases of major information security incidents.

*Bilangan pencerobohan keselamatan maklumat telah meningkat dengan drastik sedekad yang lalu. Pelbagai insiden yang berlaku membuktikan bahawa keselamatan maklumat telah menjadi isu kewangan penting yang perlu dipandang secara serius bagi melindungi nilai korporat. Polisi Keselamatan Maklumat ViTrox direka untuk melindungi rahsia, integriti, kesediaan semua aset maklumat bagi meningkatkan keyakinan pelanggan, meningkatkan daya saing syarikat serta mencegah gangguan operasi. ViTrox berusaha untuk mencapai sifar (0) kes insiden keselamatan maklumat utama.*

### Information Security Committee Organisation Organisasi Jawatankuasa Keselamatan Maklumat

1. The Management Information Security ("MIS") department is responsible for the overall planning, establishment and maintenance of the information security management system.  
*Jabatan Keselamatan Maklumat Pengurusan ("MIS") adalah bertanggungjawab dalam perancangan sistem pengurusan keselamatan maklumat, penubuhan dan penyelenggaraan secara keseluruhannya.*
2. The MIS manager takes the lead in all information security cases, establishes the information security management framework and maintains the strategy and process for protecting assets and information in the organisation.  
*Pengurus MIS menerajui semua kes keselamatan maklumat, menetapkan rangka kerja pengurusan keselamatan maklumat, mengekalkan strategi proses untuk melindungi aset dan maklumat dalam organisasi.*
3. MIS team members are responsible for planning and executing information security management, organising information security maturity assessments, as well as maintaining and implementing the Information Security Management Policy and standard operating procedure, information security risk management and information security standard compliance.  
*Ahli pasukan MIS bertanggungjawab untuk merancang dan melaksanakan pengurusan keselamatan maklumat, mengatur penilaian kematangan keselamatan maklumat, serta mengekalkan dan melaksanakan Polisi Pengurusan Keselamatan Maklumat dan prosedur operasi standard, pengurusan risiko keselamatan maklumat dan pematuhan standard keselamatan maklumat.*
4. The MIS team will report to the Risk Management Committee, one of the committees within our Board of Directors that oversees the cybersecurity strategy.  
*Pasukan MIS akan melaporkan kepada Jawatankuasa Pengurusan Risiko, salah satu jawatankuasa dalam Lembaga Pengarah bagi menyelia strategi keselamatan siber.*

### Countermeasures for Information Security Risks Langkah-langkah Mengatasi Risiko Keselamatan Maklumat

Protecting information confidentiality, integrity and availability is crucial for ViTrox's information security management. Accordingly, we identify the information security risks and work on their countermeasures.

*Melindungi maklumat sulit, integriti dan ketersediaan adalah aspek yang penting untuk pengurusan keselamatan maklumat ViTrox. Sehubungan dengan itu, kami menentukan risiko keselamatan maklumat dan berusaha mengatasinya.*

1. We regularly implement the ISO 27001 risk assessment in all facilities by designing policies in line with the ISO 27001 to uphold the highest level of information protection. We refer to the standards under ISO 27001 for our continuous improvement on information security management procedures.  
*Kami sentiasa melaksanakan penilaian risiko ISO 27001 dalam semua kemudahan dengan membentuk dasar selaras piawaian ISO 27001 untuk memperkukuhkan tahap perlindungan maklumat sedia ada pada tahap tertinggi. Kami akan merujuk kepada piawaian di bawah ISO 27001 untuk memastikan penambahbaikan dilakukan secara berterusan mengikut prosedur pengurusan keselamatan maklumat kami.*
2. We conduct educational programmes and training sessions related to information security for all employees to enhance employee awareness of the importance of information security and prevent major data breaches.  
*Kami menjalankan program pendidikan dan latihan berkaitan dengan keselamatan maklumat untuk semua pekerja bagi meningkatkan kesedaran pekerja tentang kepentingan keselamatan maklumat dan mencegah pelanggaran data utama.*

Date: 1 November 2022