MANAGEMENT APPROACH

Cybersecurity and Data Privacy

KINROSS

SUSTAINABILITY

Our Commitment

Kinross places high importance on the integrity of its information technology (IT) systems and their resilience to cybersecurity threats. Our Kinross Code of Business Conduct and Ethics ("the Code") embeds our policy expectations pertaining to the use of IT, data privacy and cybersecurity. All employees are required to comply with the Code.

Our Approach

Kinross' day-to-day business relies heavily on its IT systems, including its networks, equipment, hardware, software and telecommunications systems, as well as the IT systems of third-party service providers and vendors. As outlined in the Code, the security of Kinross Information Technology, including cybersecurity, is the responsibility of every employee.

Any suspected cybersecurity threats or incidents must be reported directly to the Kinross Information Technology department or via email at cybersecurity@kinross.com.

To help mitigate risks from increasing cybersecurity threats, we have implemented an in-depth and multi-layered defence strategy, which includes the following elements:

- IT security risk is managed globally through a centralized, risk-based methodology. Kinross' methodology is based on elements from both ISO 27001 and NIST.
- Identification and aggregation of cybersecurity risks within the Enterprise Risk Management program.
- An internal program that meets industry standards for data protection and cybersecurity protocols.
- Internal controls around the ethical use of private data.
- A classification register for each corporate function focused on maximum security for areas considered to be "high risk".
- Provision of annual cybersecurity education and training for all of its employees, contractors and the board and additional training is provided for high-risk functions within the business. Training is tailored to the needs and realities of specific functions and consists of face-to-face and interactive training tools, including via Kinross University.
- In addition to their participation in the annual on-line training via Kinross University, specific training is conducted for the Board of Directors, including in person sessions with external experts focused on cyber risk, privacy regulations and specific considerations for board and senior leadership teams.
- Collaboration with third-party service providers and vendors, including IT service providers, to help ensure that we have the resources in place to modify or enhance protective measures, or to investigate and remediate any vulnerabilities.
- Protocols for managing a breach and ensuring business continuity.

A dedicated team of IT cybersecurity professionals manage the IT security risk processes and IT security operations.

Kinross' Vice-President, Information Technology leads Kinross' IT and cybersecurity program and reports to Kinross' Senior Vice-President and Chief Financial Officer, a member of Kinross' Senior Leadership Team (Executive) who has Executive Management Responsibility for IT and Cybersecurity. The mandate of the Audit and Risk Committee (ARC) of our Board of Directors includes ongoing review of IT security risks. The ARC receives quarterly IT and cybersecurity updates from management and conducts comprehensive annual reviews of the Company's privacy and data security risks and exposures and measures taken to protect the confidentiality, integrity and availability of its management information systems and data.

For more insight on cybersecurity risk, see Kinross most recent Annual Information Form, Risk Factors.