

Data Privacy and Cybersecurity



Objective, Purpose, and Context

Kinross’ business *purpose* is to deliver value through operational excellence, balance sheet strength, disciplined growth, and responsible mining.

Our business activities are heavily dependent on our IT systems, our networks, equipment, hardware, software and telecommunication systems, as well as the IT systems of third-party service providers and vendors. Our business success depends upon meeting our responsibility to our shareholders, employees and broad range of stakeholders to maintain the integrity of our systems and resilience to cybersecurity threats, while protecting the privacy of information entrusted to us.

Our objective is to have a strong governance framework in place for cybersecurity, supported by high-quality information (IT) systems, which are resilient to cybersecurity threats. Our Kinross Code of Business Conduct and Ethics (Code) embeds our policy expectations pertaining to the use of IT, data privacy, and cybersecurity.

We have identified Data Privacy and Cybersecurity as a material sustainability topic for Kinross and a priority for the Company, of critical importance to our stakeholders and the success of our business.

This sustainability policy statement describes:

- Scope and application: who is affected and where they can find information
- Material Impacts, Risks and Opportunities (IROs) and IRO Management
- Commitments and Strategy: how we aim to meet the policy statement objective
- Governance and Accountability: who is responsible from site level to Board of Directors

Scope and Application

This policy statement applies to:

- All Kinross geographies and assets, and operations and projects
- Global upstream and downstream components of our value chain

Our stakeholders have been considered in this policy statement as described below.

Stakeholder	Policy value for stakeholders	Consideration of stakeholder in setting this policy statement
Own Workers	To provide clarity on company commitments and approach	Company values and culture
Investors/ Financial	To provide clear governance information	Outreach on Sustainability topics
Local Communities	To provide clarity on company commitments and approach	Effective management of this topic is essential for relationship quality
Media	To provide transparency about our commitments and approach	Response to requests and/or proactive outreach
Governments	To provide transparency about our commitments and approach	Adherence to applicable reporting, compliance and regulatory obligations is expected
Insurers	To provide clear governance information	Outreach on Sustainability topics
Refiners	To provide clear governance information	Through conformance with the Responsible Gold Mining Principles
Suppliers/ Contractors	To provide clarity on company commitments and approach	Through engagement on Supplier Standards of Conduct and Sustainability topics
Civil Society	To provide transparency about our commitments and approach	Through partnerships and engagement

Material Impacts, Risks and Opportunities

This sustainability policy statement relates to the following material impacts, risks and opportunities (IROs).

Impact	Risk	Opportunity
People – Data breaches to operational technology can have severe consequences for the health and safety of employees and nearby communities	Information technology disruptions, cybersecurity issues, data breaches, and hacks of operational technology can cause operational disruptions, and thus financial and reputational losses	No financially material opportunities
People – Inadequate data management throughout Kinross’ value chain can lead to cybersecurity breaches, which can violate privacy rights of stakeholders (e.g., employees and suppliers)		

IRO Management

The potential effects of material IROs pertaining to this topic and Kinross’ measures to effectively manage.

Potential Effects of Sustainability-Related Impacts, Risks and Opportunities			Short-term (1 year)	Medium (2-5) and Long-term (>5 years)
		Financial performance	Major	Major
		Society and environment	Moderate	Moderate
IRO Management	Risk Assessment	• Updated quarterly through Kinross ERM Program		
	Due Diligence	• Third-party cybersecurity assessment		
	Recognized Standards	• ISO 270001 (alignment) • National Institute of Standards and Technology (NIST)		
	Training	• End-user cybersecurity training via Kinross University – all employees “technology users”, including members of the Board of Directors • Cybersecurity training at onboarding for all new employees • Artificial Intelligence (AI) training for corporate and operating sites		
	Mechanisms for Management	• Artificial Intelligence Steering Committee • Identify and Access Governance Program		
	Monitoring and Reporting	• Quarterly reporting to Audit and Risk Committee (ARC) of the Kinross Board of Directors (internal) • Annually in Kinross Sustainability Report (external)		

Commitments and Strategy

As a senior gold company, Kinross is *committed* to the membership requirements of the World Gold Council through its **Responsible Gold Mining Principles**. This includes **Principle 2, Understanding our Impacts**, which applies specifically to data privacy and cybersecurity as it pertains to risk management (2.1 risk management).

We are also *committed* to supporting progress towards the **Sustainable Development Goals** (SDGs). Kinross is focused on **SDG 9** (Industry, Innovation, and Infrastructure), which is broadly focused on sustainable and resilient infrastructure, innovation and technology.

We rely on a robust framework for cybersecurity, combined with high-quality and resilient Information Technology (IT) systems to mitigate the risks associated with threats to our Company. Our approach to mitigating these risks is based on an in-depth and multi-layered defence strategy, managed globally through a centralized, risk-based methodology based on elements of ISO 27001 and the National Institute of Standards and Technology (NIST). We are also focused on the responsible adoption of Artificial Intelligence while also recognizing the significant opportunities for personal productivity, operational efficiency, and innovation for the Company. The key elements include:

- IT security risk is managed globally through a centralized, risk-based methodology.
- 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.
- Responsible Use Policy for Artificial Intelligence (AI) to guide workers in the safe use of generative AI, company-managed enterprise solutions, and to raise awareness about using AI securely.
- Multidisciplinary Artificial Intelligence Steering Committee (AISC), comprised of representatives from Risk, Legal and Compliance, Technical Services, IT, Human Resources, and Exploration. The AISC meets quarterly.
- 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 employees, contractors, and the Board of Directors. 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.

- Annually, conduct a comprehensive cybersecurity assessment by a third-party security firm to test the resilience of our security processes and controls against emerging cyber threats.
- Protocols for managing a breach and ensuring business continuity.

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

Metrics and Targets

We track and measure our performance in line with the metrics below and our progress against targets.

Data Privacy and Cybersecurity Metrics and Targets

Topic	Metrics	Targets
Data Privacy and Cybersecurity	• Number of material breaches related to cybersecurity • Percentage of technology users who have completed cybersecurity training	• Zero material breaches related to cybersecurity • 75% of technology users trained on cybersecurity

Governance and Accountability

Supervisory level oversight resides at the Audit and Risk Committee of the Kinross Board of Directors. Management responsibility resides with the Executive Vice-President and Chief Financial Officer. Functional responsibility for data privacy and cybersecurity resides with the Senior Vice-President, Information Technology and Artificial Intelligence.

Accountability

Reporting on performance for data privacy and cybersecurity is provided through Kinross’ annual [Sustainability Report](#).

Document control

This policy statement will be reviewed annually in parallel with our Sustainability reporting cycle to ensure it accurately describes what we do in practice to manage our Sustainability impacts, risks and opportunities. It forms an integral part of Kinross’ 2025 sustainability disclosures, approved by Board resolution on 27-May 2026, and replaces prior document – Sustainability Policy Statement, Data Privacy and Cybersecurity.



To learn more about our performance and initiatives relating to data privacy and cybersecurity, see our most recent [Sustainability Report](#).