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.

Kinross' policy statement *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 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 policy statement relates to the following material impacts, risks and opportunities (IROs):

Impact	Risk	Opportunity
On workers and surrounding community safety due to breach of operational technology	To operations from cybersecurity breaches of operational technology, causing financial or reputational loss	
On privacy of stakeholders due to inadequate use of data and cybersecurity attacks	To operations and finances from IT disruptions if systems experience extended outages	
	To reputation from data breaches causing legal issues and loss of stakeholder trust	

Note: positive IROs are italicized

This policy statement describes:

- Scope and application: who is affected and where they can find information
- Commitments and approach: how we aim to meet the policy statement objective
- Accountability: who is responsible from site level to Board of Directors

Scope and Application

This policy statement applies to all Kinross geographies and assets, operations and projects and the global upstream and downstream components of our value chain.

Continued on next page

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

Stakeholder	Policy statement effect on stakeholder	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
Communities	To provide clarity on company commitments and approach	Relationship, impacts and local benefits
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	Relationship, reporting as required and compliance with applicable regulation
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

Commitments and Approach

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

We are also *committed* to support 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).

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.
- 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.

Accountability

Functional responsibility for data privacy and cybersecurity resides with the Senior Vice-President, Information Technology and Artificial Intelligence. Management responsibility resides with the Executive Vice-President, Finance and Chief Financial Officer.

Supervisory level oversight resides at the Audit and Risk Committee of the Kinross Board of Directors.

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.

Document control

This policy statement forms an integral part of Kinross’ 2024 Sustainability Disclosures, approved by Board resolution on 27-May 2025, and replaces prior document – Management Approach Cybersecurity, dated May 2024.

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