CYBERSECURITY POLICY

POLICY BRIEF & PURPOSE

This cybersecurity policy (the "**Policy**") outlines the guidelines and provisions of Aya Gold & Silver Inc., its subsidiaries, and affiliated companies (referred to as "**Aya**" or the "**Company**") to safeguard the security of our data and technological infrastructure. In addition, this Policy sets forth Aya's expectations regarding cybersecurity practices and responsibilities applicable to all employees, consultants, directors, officers, and to the extent applicable, contractors, subcontractors, services providers, and anyone who has permanent or temporary access to our systems and hardware (collectively the "**Users**" and each, a "**User**").

As we increasingly rely on technology to collect, store, and manage information, we become more vulnerable to serious security breaches. Human errors, cyberattacks, and system malfunctions can lead to significant financial losses and jeopardize our Company's reputation.

To address these risks, we have implemented several security measures and provided guidelines to mitigate security threats, both of which are outlined in this Policy.

CYBERSECURITY FRAMEWORK

The Company is committed to maintaining the highest standards of information security across its operations. This Policy reflects Aya's proactive and comprehensive approach to information security, including its commitment to:

- ✓ **Improvement:** Continuously improving information security systems.
- ✓ **Integrity:** Ensure the integrity and protection of all data.
- ✓ **Prevention:** Implement and adhere to proactive security measures, such as secure system configurations, access controls, malware protection, authentication protocols (including two-factor authentication), network segmentation, and ongoing cybersecurity awareness, to reduce the likelihood of cyber incidents.
- ✓ **Detection:** Utilize appropriate monitoring tools and remain alert to identify suspicious activity, vulnerabilities, or threats. Awareness initiatives and periodic testing are conducted to evaluate security posture.

- ✓ **Audit:** Conduct internal audits of the information infrastructure and information security management systems;
- ✓ **Response:** Follow established incident response procedures to contain, mitigate, and escalate cybersecurity events in a timely and coordinated manner. Investigations are conducted to determine root causes and prevent recurrence.
- ✓ **Recovery and Business Resilience:** Contribute to business continuity and disaster recovery efforts to ensure that critical operations, systems, and data can be restored effectively in the event of disruption.
- ✓ **Leadership**: Establish clear individual responsibilities for information security throughout the workforce.
- ✓ **Reporting:** Provide Users with an escalation process allowing them to promptly report any actual or suspected cybersecurity incidents, vulnerabilities, or policy violations through the appropriate internal channels.
- ✓ **Third-Parties**: Establish specific information security requirements for third parties, including suppliers and service providers.

All Users are expected to actively support the Company's cybersecurity objectives across these key areas. Compliance with this framework is essential to protect the Company's systems, data, and reputation.

USERS' STANDARDS

1. Company Data

All Company data is valuable and has value that may be difficult to quantify. Company data also includes confidential information that must remain secret and not be disclosed to anyone. Examples of confidential information include:

- Unpublished financial information
- Data about our customers, partners, contractors, and service providers
- Contracts with private parties or government authorities
- Data regarding our mining operations, exploration operations, financial results
- Date and information regarding financing, possible financing, mergers and acquisitions, or partnerships.

Users must take all necessary measures to protect Company data, including confidential information, and do everything necessary to prevent security breaches.

2. Protecting Personal and Company Devices

The use of electronic devices to access Company emails or accounts poses a cybersecurity risk to our data. We ask Users to secure their personal and Company-provided computers, tablets, and mobile phones by:

- Ensuring all devices and systems are password protected, with a two-factor authenticator where possible.
- Choosing an appropriate password for all devices, software, sites and services. PASSWORD123 NAMELAST NAME type of passwords are not permitted. You must use a password which is appropriate and does not make it overly easy to guess or hack.
- Ensuring the Company provided antivirus software is up to date on your computer.
- Not leaving your devices exposed or unattended without being locked.
- Installing security updates of browsers, operating systems and software monthly or as soon as updates are available.
- Using the Company provided VPN when accessing the internet via public networks.
- Logging into company accounts and systems through secure and private networks only.

Users are requested to refrain from accessing internal systems and accounts from other people's devices or public computers (e.g. cybercafés) or lending their devices to others.

3. Annual Cybersecurity Training

All Aya employees and anyone with permanent or temporary access to our systems and hardware will receive annual cybersecurity training. This training aims to:

- Raise awareness among employees and anyone with permanent or temporary access to our systems and hardware about potential risk situations and best cybersecurity practices.
- Inform and prepare employees and anyone with permanent or temporary access to our systems and hardware to deal with emerging threats in the digital world.

This cybersecurity training is mandatory for all employees, including executives and anyone with permanent or temporary access to our systems and hardware. It will cover topics such as password protection, detecting fraudulent emails, securing personal and professional devices, secure data transfer, and other essential aspects of cybersecurity.

4. Email Security

Emails are the source of most cybersecurity incidents. Emails can contain scams, phishing attempts, and malware (e.g., Trojans) that can compromise the integrity of digital devices and Aya's overall technological network. To avoid viral infections or data theft, we ask Users to avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this incredible video", or “is it you in this picture”).

- Be cautious of clickbait subject lines (offering prizes or advice, for example).
- Be wary of emails that appear out of context or abnormal.
- Thoroughly check received emails, including the email address, electronic signature, names, and surnames to ensure they are correct.

- Pay attention to inconsistencies (e.g., grammar errors, excessive use of exclamation points, uneven characters, etc.).
- Be cautious of emails requesting changes to supplier payment information and personal information.

CAUTION: Fraudsters are skilled at creating phishing emails that closely resemble legitimate emails. The difference between a phishing email and a genuine email often lies in a few details. Therefore, vigilance is essential!

In case of doubt regarding a received email:

- Immediately report the suspicious email by clicking the "Report Phishing" button of your outlook browser, or by forwarding the suspicious email to our IT department at it@ayagoldsilver.com.
- Never respond to or forward the email to anyone except the IT department.
- Contact the person supposedly originating the email using an alternate means of communication (e.g., their phone, another email, Teams, in-person, etc.) to verify the legitimacy of the email.

5. Centralized Document Storage

To ensure the security of our computer systems and the confidentiality of our data, everything produced as part of your employment with Aya must be saved on the Company's servers. This includes contracts, geological documents, plans, engineering reports, human resources, financial, customer, supplier records, purchase orders, invoices, corporate documents, and professional emails.

It is strictly prohibited to save any documents produced as part of your employment with Aya on a server other than the Company's, including cloud storage, external platforms, your Company-provided computer's hard drive, your personal computer's hard drive, and USB drives. Failure to comply with this requirement may result in disciplinary measures in accordance with this Policy.

6. Proper Password Management

Password leaks are dangerous since they can compromise our entire technological infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we ask Users to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If Users need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, Users should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

- Choose a different password between your email password and your network and computer login password.
- Change their passwords annually.

7. Secure Data Transfer

Data transfer poses a security risk. Users must:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless absolutely necessary. When mass data transfer is required, Users must seek assistance from our IT department.
- Share confidential data on the Company's network or system, not on public Wi-Fi.
- Ensure that data recipients are duly authorized individuals or organizations with adequate security policies.
- Ensure the transfer of data to authorized third parties is done through a Company-secured data system, such as the Company's data sharing services (e.g., Company OneDrive, Dropbox), and not through personal transfer systems (e.g., personal OneDrive, WeTransfer, etc.).
- Report scams, privacy breaches, and hacking attempts.

Our IT department should be informed of scams, breaches, and malware to better protect our infrastructure. Therefore, we ask Users to report any perceived attacks, suspicious emails, or phishing attempts to our IT specialists as soon as possible. Our IT department will investigate promptly, resolve the issue, and issue a Company-wide alert if necessary.

Our IT department is responsible for advising Users on how to detect fraudulent emails, and we encourage Users to contact them with any questions or concerns.

8. Notification of Privacy Incident Involving Personal Information

A cybersecurity incident can also result in an incident involving personal information. Personal information is data that can directly or indirectly identify an individual. Examples of personal information include:

- Name
- Address
- Phone number
- Email address
- Banking information
- Social insurance number
- Medical records
- Curriculum vitae

You must promptly notify the Chief Privacy Officer of the Company of any incident involving personal information in accordance with the Privacy Policy. Contact information for the Chief Privacy Officer can be found under the section "Who to Contact Regarding This Policy?" below.

9. Additional Measures

a) What We Expect from You - In Summary

To reduce the likelihood of a cybersecurity incident, we ask Users to:

- Turn off their screens and lock their devices when leaving their desks, even momentarily.
- Change passwords for all accounts when a device is stolen or lost.
- Report any of the following:
    - Stolen or damaged equipment to their supervisor and our IT department as soon as possible.
    - perceived threats or security weaknesses in the Company's systems to our IT department.
    - incidents of personal information privacy breaches to the Chief Privacy Officer.
- Refrain from downloading suspicious, unauthorized, or illegal software onto Company-owned computer equipment.

b) Social Media & Internet Usage Policy

Users must also comply with our Social Media and Internet Usage Policy.

c) Responsibility of the IT Department

Our IT department must:

- Install firewalls, antivirus software, anti-malware software, and access authentication systems.
- Regularly inform Users about new fraudulent emails or viruses and how to combat them.
- Conduct thorough investigations into security breaches.
- Adhere to the provisions of this policy, as Users do.
- Avoid accessing suspicious websites.

10. Remote Users

Remote Users must also follow the instructions in this Policy. Since they access Company accounts and systems remotely, they are required to adhere to all encryption and data protection standards and ensure the security of their private network.

We encourage all Users to seek cybersecurity advice from our IT department at the contact provided under the section "Who to Contact Regarding This Policy?" below.

DISCIPLINARY MEASURES

This Policy must be followed and respected by all Users. Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment or contract. For employees, any violation of this Policy will result in disciplinary measures, including:

- First offense, unintentional or minor violation: verbal warning and the requirement for the employee to review cybersecurity policies, undergo cybersecurity training, and review cybersecurity training materials.
- Subsequent offenses, intentional violations, repeated violations, or major violations (causing significant harm): More severe disciplinary measures may be applied, including termination. Each incident will be reviewed on a case-by-case basis.

An employee may face disciplinary measures for violating or failing to comply with this Policy even if it does not result in a security incident.

INCIDENT REPORTING AND ESCALATION PROCESS

All Users are responsible for reporting any actual or suspected cybersecurity incidents, system vulnerabilities, or suspicious activities without delay. Reports must be made through the designated internal reporting channels, such as the IT helpdesk or the anonymous reporting platform via the process established by the Whistleblowing Policy.

The Company has implemented an escalation process to ensure that all reported issues are assessed based on severity and promptly directed to the appropriate level of management or response team. Users must cooperate fully during the investigation process and follow any guidance provided by the cybersecurity or compliance teams. Failure to report or escalate such incidents may result in disciplinary action, up to and including termination of employment or contract.

TAKE CYBERSECURITY SERIOUSLY!

All of our partners, whether customers, contractors, employees, or subcontractors, should have confidence that their data is secure. The only way to earn this trust is by proactively protecting our systems and databases. We can all contribute to this by being vigilant and making cybersecurity a priority!

WHO TO CONTACT REGARDING THIS POLICY?

General

For any questions regarding this Policy:

- Elias J. Elias, Chief Legal and Sustainability Officer

- elias.elias@ayagoldsilver.com

Personal Information

For any questions regarding personal information protection or to report a personal information incident:

- Privacy Officer
- privacy@ayagoldsilver.com

IT Department

To seek cybersecurity advice or report cyberattacks, suspicious emails, or phishing attempts:

- it@ayagoldsilver.com

Last Updated: May 2025

Approved by the Environment, Social and Governance Committee of the Board of Aya Gold & Silver Inc.