CYBERSECURITY POLICY

---

1. POLICY BRIEF & PURPOSE

Our company's cybersecurity policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

2. SCOPE

This policy applies to all our employees, employees of subsidiaries and affiliates, contractors and anyone who has permanent or temporary access to our systems and hardware.

3. POLICY ELEMENTS

A. Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/contractors/service providers
- Private contracts or government agreements, geological and technical data
- Data regarding our mining operations, exploration operations, financial results
- Date and information regarding financings, possible financings, mergers and acquisitions, partnerships, etc.

All employees should take all necessary steps to protect all company data, including specifically confidential information and do all that is necessary to avoid security breaches.

B. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this 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.
- Keeping all devices password protected.
- Ensuring the company provided antivirus software is up to date on your computer.
- Ensuring not leave their 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.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices, public computers (e.g. internet café), or lending their devices to others.

C. Keep emails safe

Emails often host scams and malicious software (e.g. trojan horses.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email addresses and names from the sender they received a message from to ensure they are legitimate and in case of doubt do not reply or text back but start a new conversation with the person you suspect this is from using a method of communication you know is theirs (their phone, other email, Teams, in person, etc.)
- Look for inconsistencies or clues (e.g. grammar mistakes, capital letters, excessive number of exclamation marks, etc.)

If an employee isn't sure that an email they received is safe, they can refer to our IT department at it@ayagoldsilver.com

D. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, ask our employees 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 employees 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, employees 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/computer login password.
- Change their passwords every year.

E. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT service for help.
- Share confidential data over the company network/ system and not over public Wi-Fi.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Ensure to data to authorized 3rd parties is done via a company system which provides data security such as the company's data sharing services (e.g. company one-drive, Dropbox) and not via a personal transfer system (e.g. personal one-drive, we transfer, etc.)
- Report scams, privacy breaches and hacking attempts

Our IT service provider needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we ask our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our specialists. Our IT service provider will promptly investigate, resolve the problem, and send a company-wide alert if necessary.

Our IT service provider is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

F. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to their manager and IT service provider.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

Our IT service provider should:

- Install firewalls, anti-virus, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

G. Remote employees

Remote employees must also follow this policy's instructions. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT service provider.

4. DISCIPLINARY ACTION

We expect all our employees to follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and ask that the employee review policies on security and/or review security training material.
- Intentional, repeated, or large-scale breaches (which causes financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity top of mind.