CAPSTONE
COPPER

CYBER SECURITY FACT SHEET

1. OVERVIEW

Cyber security is a strategic business matter for Capstone Copper Corp ("Capstone" or the "Company"). Therefore, it is committed to achieving a targeted level of protection from cyber and information security threats.

The assessment and management of cyber and information security risk is integrated into our Enterprise Risk Management (ERM) System. Capstone's robust ERM System is implemented across Capstone to ensure that the risks affecting Capstone's business objectives and strategy are identified, evaluated, and managed. Capstone highlights the importance of cyber and information security risk through direct oversight from the Board of Directors.

Capstone's ERM Framework includes the establishment of cross functional management committees to manage key risks to the company. The Global Cyber Security Committee manages information security risk through ongoing governance, policies, practices, and cyber security training initiatives. Capstone continuously monitors the effectiveness of existing controls and the Cyber Incident Response Plan and utilizes third parties to assist with identifying and assessing new cyber threats and system vulnerabilities.

Capstone's global Cyber Security Policy defines Capstone's commitment to embedding Capstone's cyber security practices across all levels of the company and business activities. The Cyber Security Policy applies to all permanent and temporary employees ("employees") of Capstone and all subsidiaries, and to directors, Suppliers, and other users of Capstone's IT resources (together referred to as "system users") wherever they may be located.

2. CAPSTONE'S COMMITMENTS

Capstone and all subsidiaries are committed to achieving a targeted level of protection from internal and external cyber and information security threats, and accordingly, will implement ongoing governance, policies, and practices which address the following objectives:

- Ensure compliance with all applicable laws, regulations, and Capstone's policies, controls, standards, and guidelines.
- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach.
- Comply with requirements for confidentiality, privacy, integrity, and availability for Capstone's Suppliers[1], and other users.
- Establish controls for protecting Capstone's information and information systems against theft, abuse, and other forms of harm or loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security.
- Ensure the protection of Capstone's data and information assets.

[1] "Supplier" means any person, corporation or other legal entity that provides goods or services to or on behalf of Capstone. This includes goods and services delivered to and used on Sites; or required to transport Products to markets. Suppliers includes consultants, vendors, contractors, and agents.

- Ensure the availability and reliability of the network infrastructure, systems and the services.

- Ensure that Suppliers are made aware of, and comply with, Capstone's information security needs and requirements and continuously assess whether they maintain an acceptable cyber security posture.

- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility.

- Regularly assess developments within the company and in the environment, and ensure the promulgation of corporate wide policies for:

  - Cyber security management,
  - Management of third party's access to company networks, and
  - Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threat.

3. EMPLOYEE AND SYSTEMS UNDER COMMITMENTS

All employees are provided with adequate technology, data and information access as required and where relevant to perform their responsibilities. All employees and system users at Capstone are required to securely and appropriately use, safeguard, and protect all technology, data, and confidential information against the risk of damage, loss, theft, alteration, and unauthorized access.

Capstone prohibits its employees and system users from using company provided technology, information and data to commit unlawful practices including cybercrime, duplicating or selling software or media files, using non-licensed software, sharing of passwords, using technology or data for non-business purposes or with the intent to cause reputational damage to Capstone or others. To maintain the integrity of Capstone's corporate image and reputation and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential or personal information, employees must exercise caution and care when using any system, service or technology platform, both internal and external, including email or third-party services.

4. TRAINING AND DEVELOPMENT

Cyber security training and awareness sessions are provided as an integral part of employee onboarding and ongoing employee development. Our cyber training program extends to the Board of Directors.

In addition, acknowledgement of the Cyber Security policy, that it is understood, and that the employee agrees to apply it is included in the annual sign off along with the Code of Conduct. Training is conducted on the Code of Conduct biannually with testing performed on the alternating year. The objective of the cyber training program is to minimize human element cyber risk.

5. REPORTING AND INCIDENT RESPONSE

Cyber Security threats are promptly reported and managed in accordance to the Cyber Incident Response Plan. The Cyber Incident Response Plan is an extension of the Crisis Management Plan and is comprised of a cross-functional Response Team. Capstone has not experienced an information security breach to date.

Corporate IT is responsible for the development and promulgation of standards and guidelines for acceptable IT related business continuity and disaster recovery plans globally. Our business continuity and disaster recovery plans, including data backup and recovery, are developed for the global IT environment, network, infrastructure, and services and applications' software for each operating unit or office. The business continuity plans are tested periodically. The results of these tests are documented and promptly addressed.

Cyber security management is reflected in reports and updates to operations management and senior management. The Board of Directors are briefed quarterly on cyber and information security matters and risks and as deemed necessary by the Cyber Incident Response Plan.