# INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY

This Information Technology and Cybersecurity Policy (the "**Policy**") is meant to protect District Metals Corp.'s (together with its subsidiaries, the "**Company**" or "**District**") data and infrastructure, outline guidelines that govern cybersecurity measures and define information technology ("**IT**") infrastructure usage.

The Policy applies to District, its subsidiaries and affiliates, and all directors, executive officers, employees and consultants of District (collectively, "**District Personnel**").

## Policy Scope

- User access to District's IT infrastructure is provided to District Personnel to facilitate productivity and assist them to effectively perform their duties and responsibilities within the Company.
- The Company assigns laptops or desktops and associated hardware and software to District employees, and requires that the hardware and software be used for conducting Company business. All users of District technology must respect the intended business use of the technology, and comply with all applicable software licenses, property rights and user agreements and other similar agreements or third party imposed terms and conditions..
- District expects District Personnel to strictly comply with the Company's Code of Business Conduct and Ethics, and all applicable law when using the IT resources. This also includes respecting privacy and intellectual property laws.
- District expects District Personnel to be responsible for creating unique passwords that are safeguarded against any inadvertent access. The minimum password length should be 8 characters with a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and symbols. The password should not be identical to account name or email address. Passwords are to be changed every 6 months.
- Email usage by District Personnel should be treated in the same manner as any other form of communication. Users must exercise caution when sending email. Sensitive information must not be forwarded unless that email is critical to business. The content of email should be in accordance with the conduct outlined in the Company's Code of Business Conduct and Ethics.
- District Personnel are encouraged to scrutinize all emails before clicking links or responding. All users must report any suspicious email they are suspicious of before they take any further action to the Company's external IT consultant or the Company's Chief Financial Officer ("CFO").
- All material prepared or received by District Personnel that relates to the Company's business is expected to be stored on the Company file servers.
- Access to District data and information is reviewed and monitored by the Company's Chief Executive Officer ("CEO"), CFO and Vice President Exploration, if applicable.

- Security breaches must be reported immediately to the Company's external IT consultant or the Company's CEO or CFO. The issues must be documented, including any follow-up after the incident.
- District Personnel will be offered continuing education in cybersecurity in order to better understand and evaluate the Company's preparedness and District Personnel.

## Review of this Policy

The Board recognizes that the policy is an evolving area in Canada and globally and will review this policy annually to ensure that it is effective in achieving its objectives and that the Company's practices continue to be representative of sound corporate governance practices.

## Effective date

This Policy was adopted by the Board of Directors on June 7, 2024.