corporate policy

Subject: Cybersecurity Policy

Corporate Policy No**. XXX** Date Issued: **January 31, 2020**

Application:	This Policy including Schedule "A" ("Policy") governs all personnel, including employees, contractors and consultants of the Company.

1.0 Purpose

To set out mandatory standards for protection of Company Information, in accordance with applicable laws and regulatory requirements.

2.0 Principles

The underlying principles of this Policy are:

- Company Information, assets and resources, especially sensitive data, must be protected from unauthorized access, modification, destruction or disclosure, including by compliance with all Security Standards;
- Any impact to the Company resulting from security incidents must be mitigated and managed in accordance with the Security Standards; and
- The company's brand and reputation must be protected from any negative impact or publicity resulting from security incidents.

3.0 Definitions

(a) *"***Company Information***"* means emails, messages, documents, data and other information, including personal health information, customer data and colleague records, regardless of physical form or characteristic (including paper, electronic, audiovisual, etc.), which are created, sent, received, reproduced, processed, stored, transmitted or maintained by personnel in the performance of their duties for the Company.

(b) *"***Contractors***"* means persons contracted by the Company to supply goods or services. This includes business entities.

(c) "**Information**" means Company Information and Non-Company Information.

(d) "**Information Security**" means measures and standards to protect Company Information and assets.

(e) "**Non-Company Information**" means emails, messages, documents, data and other information, regardless of physical form or characteristic (including paper, electronic and audiovisual), which are created, sent, received, reproduced, processed, stored, transmitted or maintained by personnel for personal use.

(f) *"***Security Controls**" means measures in the Security Standards, which are required to protect Company Information, such as passwords, access restrictions and encryption.

(g) "**Security Standards**" means mandatory security requirements contained in Schedule "A".

4.0 Process and Implementation

4.1 All personnel must:

- Comply with the Security Standards and implement security controls;
- Conduct their work in a manner that complies with the Principles set out above;
- Complete mandatory Information Security awareness training, as required; and
- Promptly report to their managers all cases where Company Information may be at risk of misuse, damage or misappropriation.

4.2 In order to implement and ensure compliance with this Policy:

a) The Chief Executive Officer must:
- Bear overall responsibility for governance of the Cybersecurity program at the company; and
- Review and approve or amend Information Security policies and procedures, based on recommendations from the Cybersecurity group, and/or Audit team.

b) The Cybersecurity group must:
- Implement effective strategies to limit the risk of misuse, damage and misappropriation of Information;
- Coordinate the creation and implementation of Information Security policies, procedures, standards and other control processes that meet the business needs of Sparkrock;
- Create awareness of the Security Standards and Security Controls;
- Provide consultation services to various business units (BUs) and functional groups and recommend risk mitigation strategies; and
- Ensure that periodic reviews of the Cybersecurity program are completed and set out in the Security Standards, and that the results of such reviews are reported to the leadership of affected BUs.

c) All Leaders must:
- Plan and budget for business initiatives in compliance with this Policy; and
- Ensure that their BUs use Information systems and assets only in compliance with this Policy.

d) All Managers must ensure that their direct reports (including Contractors and consultants):
- Understand and comply with this Policy; and
- Have access to information and information systems only to perform their assigned job functions.

5.0 Compliance

Any personnel who fail to comply with this Policy are subject to disciplinary action up to and including termination of employment or contract, and/or legal proceedings.

6.0 Reference Documents

- Security Standards (Schedule “A”)
- Acceptable Use of Company IT Assets Policy
- Code of Conduct
- Privacy Policy

7.0 Interpretation

The Chief Executive Officer has responsibility for interpretation of this Policy.

8.0 Review

This Policy will be reviewed annually or earlier where required.

Approved by:

_____
Chief Executive Officer