INDROCORP TECHNOLOGIES INC. DBA INDROTEK
(the "**Corporation**")

CYBERSECURITY POLICY

Purpose

The purpose of this Cybersecurity Policy (or the "**Policy**" as the context provides for) is to serve as a standard for setting, reviewing and implementing the Corporation's cybersecurity goals, objectives and targets.

The information that exists within the information technology ("**IT**") network and infrastructure (the "**Cyberspace**") is a valuable asset of the Corporation and, therefore, benefits from protection and preservation thereof. Effective information security management is necessary for the secured sharing and protection of information within the Corporation's Cyberspace.

This Policy serves as a framework that all employees, directors and officers shall abide by to ensure that risks to the confidentiality, integrity or availability of the Corporation's assets within the Cyberspace are managed in accordance with the agreed upon cybersecurity approach. In guiding the Corporation's ongoing operation, maintenance and effective management of its cybersecurity initiatives, this Policy will detail the roles and responsibilities of key personnel, provide guidance on the initiatives necessary to meet the objectives of this Policy, and support the Corporation in working towards its Center for Internet Security ("**CIS**") maturity target of 1.8-2.5 while minimising the Corporation's exposure to cybersecurity risks.

Applicability

This Policy applies to all directors, officers, employees and contractors of the Corporation and any parent, holding companies and subsidiaries regardless of the terms of their contract (collectively, "**you**"), who use the Corporation's technological devices. References in this Policy to "**we**", "**us**" or "**our**" shall be interpreted as referring to the Corporation unless the context suggests otherwise.

Policy Statement

The Corporation recognizes the importance of effective information security management and strives to maintain the confidentiality, integrity and availability of information in the Cyberspace. In aspiring to prevent, detect and respond to unauthorized and malicious attacks in the Cyberspace, the Corporation will identify, prioritize and manage dedicated efforts towards both protection of information and the minimization of risks of unauthorized and malicious access to information in the Cyberspace.

The Board of Directors of the Corporation (the "**Board of Directors**") aims to lead the Corporation in a direction that minimizes the risk of unauthorized and malicious use, disclosure, potential theft, alteration or damaging effects of the Corporation's operations while concurrently enabling the

sharing of information in Cyberspace. The Board of Director is committed to ensuring that risks to the confidentiality, integrity or availability of Corporation-owned information assets are managed and appropriately by implementing an information security risk management approach support by the incorporation of the CIS Controls. In furthering the Corporation's mission to protect information within Cyberspace as a valuable asset, the Corporation is committed to its information security program aimed at securing the information asset of the organisation. In addition, the Corporation strives to ensure continued protection and maintenance of a secure environment for users of its Cyberspace information by aligning its information security approach with the CIS Controls and Industry standards. This includes reserving a right to monitor and audit network and system usage at any time for compliance reasons pursuant to this Policy. The Corporation views all reports of breaches hereunder seriously and will abide by rigorous investigation processes in the event of a breach.

Roles and Responsibilities

Team leads from various departments of the Corporation have been identified under this Policy to report to the Corporation's Chief Financial Officer (the "**CFO**") and oversee the Strategy (as defined herein) of the Corporation. While these named leaders will oversee the Strategy pursuant to this Policy, cybersecurity is the responsibility of all business stakeholders and requires the cooperation and compliance of all personnel.

Employee Responsibility

All employees shall exercise professional judgement in using computing devices and network resources connected to the Cyberspace. All information, physical and intellectual properties stored on electric and computing devices or existing within the Cyberspace remain the sole property of the Corporation. Therefore, employees must neither access nor share confidential and proprietary information prior to receiving consent from management or the Corporation's directors and officers.

Employees are strictly prohibited from performing any act that would be in contrary to this Policy, including but not limited to:

- accessing data, a server or an account for any purpose other than conducting the Corporation's business in ordinary course;
- copying or distributing copyrighted material or intellectual property without prior consent;
- installing any copyrighted software without obtain approval from the Corporation's third party IT group;
- sharing passwords with other individuals or allowing others access to your accounts;

- exporting software, technical information, encryption software or technologies prior to obtaining consent from either management or the Corporation's third party IT group; and
- making fraudulent offers of products, items or services from any account that represents the Corporation.

All potential threats or loss of any Corporation device that may store confidential information must be promptly reported to the CFO.

Management Responsibilities

First and foremost, the Corporation's management team shall facilitate an environment whereby managing cybersecurity risk is accepted as the personal responsibility of each member of the Corporation. Management will consist of the following roles and responsibilities:

- IT Manager:
  - Penetration Testing Program;
  - Data Flow Enforcement;
  - Network Segmentation;
  - Secure Application Development Standards;
  - Unified Users & Group Definitions;
  - Data Protection (VPN); and
  - Privileged Access Management.
- Security Subject Matter Expert:
  - Asset Management;
  - Web Content Filtering;
  - Endpoint Hardening;
  - Email Security;
  - Security Monitoring;
  - Data Leakage Prevention;
  - Mobile Device Management;

- Incident Response Program;
- Disaster Recovery Program; and
- Patch & Vulnerability Management.

- Risk:
  - IS Governance, Policies and Standards;
  - Cybersecurity Risk Management;
  - Deficiencies and Deviation Management; and
  - Strategic Metrics and Reporting.
- Legal:
  - Coordinating Audit/Regulatory Exercises;
  - Information Security Compliance; and
  - Forensics.
- Human Resources:
  - Awareness and Training Program;
  - Knowledge and Talent Management; and
  - Background Screening.
- Finance:
  - Third Party Risk Management Program.
- Facilities:
  - Physical Security Improvements.

Management will ensure that employees are provided with adequate resources and trainings to fully understand the guidelines and expectations for cybersecurity. Members of the management team may be asked by the CFO to assist with IT security investigations in the event of a breach of this Policy. If any member of management is unaware of the best course of action in dealing with an IT-related matter, the manager shall immediately contact the Corporation's third party IT representative. Upon becoming aware of a potential violation of this Policy or a breach of

cybersecurity, the member of management must immediately document the violation and request the individual surrender possession of any devices that may have suffered a security breach.

Board of Directors

The Board of Directors of the Corporation (the "**Board of Directors**") will be responsible for, among other things, reviewing this Policy and developing recommendations for improvements and updates periodically.

The Board of Directors shall be responsible for developing measurable objectives to implement this Policy and to measure its effectiveness. The Board of Directors shall also discuss and agree annually on whether to set targets based on industry guidelines and principles published by the industry and lawmakers alike.

The Board of Directors shall monitor, on an ongoing basis, the implementation and effectiveness of this Policy and shall, annually or otherwise when applicable, assess (i) applicable legislation, regulations and guiding principles, (ii) the measurable objectives set pursuant to this Policy and (iii) progress in achieving such measurable objectives, including any targets, if set.

Cybersecurity Initiatives

The Corporation's cybersecurity strategy (the "**Strategy**") consists of 21 cybersecurity initiatives intended to drive the Corporation towards achieving its cybersecurity goals. While all initiatives are pragmatic and practical for the Corporation to implement, the Corporation will focus on five important initiatives that have a superior combination of achievability, limited dependencies and risk reductions:

1. Short to Medium Term Cybersecurity Target Operating Mode (TOM);
2. Email Security;
3. Unified Users and Group Definitions;
4. Mobile Device Management; and
5. Endpoint Hardening.

Each initiative shall have accompanying documentation prepared to formalize the operations and its links to this Policy. The initiatives will be placed into four time-frame categories: (i) Immediate Term (0-12 months); (ii) Medium Term (12-24 months); (iii) Long Term (25-36 months); and (iv) Beyond. Each initiative is further organized by complexity as follows: (a) High (will most likely require new headcount or temporary resources – specialist needed); (b) Medium (potential for new headcount or temporary resources – specialist recommended); and (c) Low (most likely can to be done with existing resources). Accordingly, the initiatives are to be written in the following format: "x. Initiative → Complexity, Time Frame", with asterisk (*) indicating a dependency. The 21 initiatives are as follows:

Immediate Term (0-12 months)

- Email Security → Medium, 0-3 months;
- Unified Uses & Group Definitions → High, 0-6 months;
- Mobile Device Management → Medium, 0-3 months;
- Endpoint Hardening → Medium, 3-9 months;
- Data Protection (VPN)* → Low, 6-9 months;
- Asset Management (Workstations, Servers and Networks) → Phase 1 (Low, 6-9 months) and Phase 2 (High, 18-24 months); and
- Web Content Filtering* → Medium, 9-16 months.

Medium Term (12-24 months)

- Incident Response Program → Low, 9-14 months;
- Network Segmentation → High, 18-25 months; and
- Disaster Recovery Program → Low, 15-18 months.

Long Term (24-48 months)

- Patch and Vulnerability Management → High, 24-31 months;
- Security Monitoring → High, 24-38 months; and
- Awareness and Training Program → Medium, 0-36 months.

Beyond 3 Year Strategic, Flexible Schedule

- Privileged Access Management → High, 36-42 months;
- Data Flow Enforcement → Medium, 36-48 months;
- Secure Application Development Standards → Low, 49-51 months;
- Data Leakage Prevention → High, 49-62 months;
- Asset Management (Software) → Medium, 49-55 months;
- Third-Party Risk Management Program → Low, 62-65 months;

- Physical Security Improvements → Medium, 62-69 months; and
- Penetration Testing Program → Medium, 62-69 months.

CIS Controls

To ensure the continued protection of the Corporation and to maintain a secure environment for its users, the Corporation strives to align its cybersecurity approach with the CIS Controls and industry standards:

Basic CIS Controls

- Inventory and Control of Hardware Assets;
- Inventory and Control of Software Assets;
- Continuous Vulnerability Management;
- Controlled Use of Administrative Proceedings;
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers; and
- Maintenance, Monitoring and Analysis of Audit Logs.

Foundational CIS Controls

- Email and Web Browser Protections;
- Malware Defenses;
- Limitation and Control of Network Ports, Protocols and Services;
- Data Recovery Capabilities;
- Secure Configuration for Network Devices, such as Firewalls, Routers and Switches;
- Boundary Defense;
- Data Protection;
- Controlled Access Based on Need to Know;
- Wireless Access Control; and

- Account Monitoring and Control.

Organizational CIS Control

- Security Awareness and Training Program;
- Application Software Security;
- Incident Response and Management; and
- Penetration Tests and Red Team Exercises.

Restrictions and Limitations

Individuals who are subject to this Policy are not limited to the restricted use of specific devices. This Policy is all encompassing and incorporates all future and personal devices that may be used to store IT and confidential information of the Corporation, including intellectual property.

Enforcement

Failure to comply with this Policy or support this Policy and the mandates herein may compromise the Corporation's information assets and cause irreparable harm to the organisation, its people, clients and digital and physical assets. For further clarity, violations of this Policy may include, but are not limited to, the conscious release of data or confidential information to unauthorized parties, conscious downloads of software or hardware that jeopardizes the security of the Corporation, and openly sharing passwords with any individual. Violations or breaches of this Policy or the associated schedules, standards or guidelines may result in suspension, discipline up to and including termination, in addition to administrative sanctions or legal actions.

Compliance Contacts

If you have any questions respecting this Policy, please contact the Corporation's CFO.

_____