

**NORTHERN CASKET (1976) LIMITED** (the “Employer”)

<b>Department:</b>	Human Resources/Employee Relations	<b>Issued:</b>
<b>Subject:</b>	<b>ELECTRONIC MONITORING POLICY</b> (this “Policy”)	<b>Effective:</b> October 11, 2022
<b>Issue to:</b>	All Employees	
<b>Issued by:</b>	Caley Ferguson, President	<b>Pages:</b> 5

**1. Purpose:**

- 1.01. The Employer may monitor any electronically administered systems for the purpose of protecting the Employer’s confidential information and reserves the right to protect these assets for a variety of reasons, such as (but not limited to) backing-up important information, to find lost data, to comply with an investigation of wrongful acts or to recover from a system failure, to participate in a system audit, or to ensure that employee use of information does not interfere or conflict with the Employer’s normal operational or business objectives.
- 1.02. The Employer may utilize electronic equipment or security systems to monitor its physical workplace premises to ensure the physical security, integrity, and safety of our employees and any physical assets situated on our physical premises.
- 1.03. The Employer may utilize electronic systems administered by the Employer to ensure that the conduct of employees during the course of employment, including employment duties performed remotely or outside of the Employer’s physical premises, are consistent with the Employer’s normal operational or business objectives.
- 1.04. All information monitored or collected through electronic means is securely stored and protected. If any personal information is collected, its use and disclosure is limited to the stated purpose(s) for its collection. The Employer continues to adhere to all privacy and confidentiality regulations, as well as prudent best practices.

**2. Monitoring of Electronic Systems**

- 2.01 The internal electronic systems of the Employer are the Employer’s assets and critical components of our communications infrastructure which we may need to monitor or retrieve contents from for the Employer’s organizational purposes.

### 3. Electronic Monitoring Practices

3.01 The Employer utilizes the following electronic monitoring practices (checked as applicable):

	<b>Monitoring Practice</b>	<b>Description</b>	<b>Purpose</b>
	Access to Workplace Server	The Employer may monitor an employee's use of its workplace (cloud) server, including internet usage, application usage, long on/off times during remote access sessions outside of the physical premises of the Employer.	1.01 1.03
	Employer Email or Instant Messaging System	The Employer may monitor employee communications on any of its software or hardware systems, including during remote access sessions (if applicable).	1.01 1.03
	Employer Provided Mobile Phone, Laptop, Computer or Other Device(s)	The Employer may monitor employee text messages, internet browsing and application usage on its mobile phone, laptops, computers or any other electronic device.	1.01 1.03
	Video Surveillance and Security Systems	The Employer may monitor its physical premises using visual surveillance or any type of electronic security system.	1.02
	Employee Time & Attendance System	The Employer may monitor an employee's work time using an electronic time recording system.	1.03
	Employee Access to Physical Premises	The Employer may utilize an electronic system to permit and record employees' access to its physical premises through access cards, key fobs or other devices.	1.02 1.03
	Global Positioning System Tracking - Employer Vehicle	The Employer may utilize GPS tracking systems in any of its motor vehicles.	1.03

### 4. Privacy and Passwords

4.01 All e-mail messages, content, images and/or attachments contained in an email address administered by the Employer are the property of the Employer, therefore employees should not expect that they are private.

- 4.02 Employees should be aware that deleted files may be retrieved and read by the Employer.
- 4.03 The Employer reserves the right to retrieve, monitor, disclose or review any messages, content, images or attachments within our internal systems for any purpose identified in this Policy herein, without notice to the employee and without seeking permission of the employee.
- 4.04 Computer or other electronic device passwords are the property of the Employer and must be disclosed to Management upon request.
- 4.05 Users expressly waive any right of privacy in anything they create, store, send or receive on the Company's computer system.

## 5. **Employer Property**

- 5.01 In addition to system hardware and software, all electronic files, data, templates, media and e-mail messages are the property of the Employer, whether composed, received or sent by the employee.
- 5.02 E-mail messages and other electronic files contained within an email address administered by the Employer constitute business records belonging to the Employer.
- 5.03 The Employer retains the right to access, copy and change, alter, modify, destroy, delete or erase this property without prior notice to employees.

## 6. **Video Surveillance**

- 6.01 Video surveillance does not include electronic audio surveillance.
- 6.02 It is forbidden for unauthorized employees to handle, view or manipulate any video surveillance equipment or related software.

## 7. **(Deemed) Compliance with Applicable Legislation:**

- 7.01 Notwithstanding this Policy, or any provision(s) or part(s) of this Policy, if:
  - (a) any provision or requirement of this Policy violates, or potentially violates; and/or
  - (b) for any employee(s), a greater, or superior, right, benefit or entitlement is granted, conferred or required by,
    - (i) the *Employment Standards Act, 2000*, SO 2000, c. 41, as amended (the "Act");
    - (ii) the (Ontario) *Occupational Health and Safety Act*, R.S.O. 1990, c. O.1, as amended (the "OHSA");
    - (iii) the (Ontario) *Human Rights Code*, R.S.O. 1990, c. H. 19, as amended (the "Code");

- (iv) the (Ontario) *Workplace Safety and Insurance Act, 1997*, S.O. 1997, c. 16, Sch A, as amended (the “WSIA”); and
- (v) every other applicable municipal, provincial or federal legislation in effect currently, or in future, as amended, including any regulations thereto (collectively, the “Legislation”),

the Legislation, as may apply, shall always govern and prevail over this Policy and be strictly adhered to by the Employer and, for greater certainty, every employee of the Employer shall always be entitled to every protection, right, benefit and entitlement required by the Legislation, as may apply, regardless of this Policy and any of its provisions. Under no circumstances shall any employee of the Employer ever be deprived of, denied or otherwise not be provided by the Employer, any right, benefit and entitlement required by the Legislation, as may apply, notwithstanding any provision(s) of this Policy and, for even greater certainty, any such right, benefit and entitlement required by the Legislation, as may apply, shall be deemed to be incorporated into this Policy by reference, and be substituted for any offending, violative or non-compliant provision(s) of this Policy.

**8. Revisions and Updating - Additional Electronic Monitoring Practices:**

Monitoring	Description	Purpose	Applicable Date

**9. Revision Updating and Control:**

Date:	Revision:	Effective: