Information Technology	Document No.	Revision Level:	
Description: **BRING YOUR OWN DEVICE (BYOD) POLICY**	**Issuer: Christopher Vanco**		
	Revised By:		**Revision Date:**

1.0 PURPOSE

Zippo Manufacturing Company, W.R. Case & Sons Cutlery Company and Northern Lights Enterprises, Inc. ("Company") permits eligible employees to use their own personal electronic devices, including but not limited to smartphones, tablets, mobile phones, and cellphones (" devices"), to perform work for Company or on Company's behalf. However, to protect Company and its employees, any use of a device for business purposes must conform to this policy as described below. In addition, each user is responsible for using their device in a sensible, productive, ethical, and lawful manner.

This policy (sometimes referred to as the BYOD policy or program) applies to work performed on a device on Company's behalf during working and nonworking hours, on and off of Company's premises.

2.0 ELIGIBILITY

A limited number of employees may be eligible to receive a company-provided standard edition (SE) iPhone. Those eligible to receive a company-provided phone are the following (subject to executive-level approval):

1. Employees who communicate via mobile phone extensively with external customers (this category of employee is not eligible for BYOD because the Company will need to retain the phone number)
2. Employees who travel extensively for work (more than 33% of the time)
3. Employees who are on call or whose duties require them to be available outside of normal business hours

Employees who are eligible to use their own device under this BYOD Policy include (a) any employee who is eligible to receive a company-provided device but would prefer to use their own device (except those in category 1), and (b) other employees whose Supervisor deems it to benefit the Company to be able to answer emails or calls outside of normal business hours and while away from their computer. For clarity, a broader set of employees may be eligible for the BYOD program than who are eligible for a company-provided device.

3.0 PROCEDURES FOR ENTERING BYOD PROGRAM

Employees may enter the BYOD program in the following ways:

1. New employees:
    a. The hiring Supervisor must indicate on the staff requisition form and the IT new hire form whether a new employee is (a) eligible for a company-provided device only (e.g., category 1 above); (b) eligible for their choice of a company-provided device or BYOD; (c) eligible for BYOD only; or (d) not eligible for any device or BYOD.
    b. If the new employee is eligible for (as indicated on the staff requisition form) and chooses (as determined during the onboarding process) the BYOD program, HR will obtain a BYOD form from the new employee.
    c. HR will maintain the completed BYOD form in the employee's personnel file and submit the employee's name to finance and to IT.
    d. Finance will arrange for the stipend payment.
    e. IT will arrange for the appropriate software to be obtained and installed on the BYOD device.

2. Replacements:
    a. IT will offer current employees who are eligible for replacement devices their choice of a company-provided device or the BYOD program.
    b. If the employee chooses the BYOD program, IT will refer the employee to HR for the BYOD form.
    c. HR will obtain a completed BYOD form from the employee.
    d. HR will maintain the completed BYOD form in the employee's personnel file and submit the employee's name to finance and to IT.
    e. Finance will arrange for the stipend payment.
    f. IT will arrange for the appropriate software to be obtained and installed on the BYOD device.

4.0 NO EXPECTATION OF PRIVACY

All material, data, communications, and information, including but not limited to email (both outgoing and incoming), telephone conversations and voicemail, instant messages, and internet and social media postings and activities created on, received, or transmitted by, printed from, or stored or recorded on the device for Company's business or on behalf of Company (" Company content") is the property of Company, regardless of who owns the device(s) used.

You are expressly advised that in order to prevent misuse, Company reserves the right to monitor, intercept, review, and remotely wipe, without further notice, all Company content, in Company's sole discretion. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, and other uses of the device, whether the device is in your possession or Company's possession. Therefore, you should have no expectation of privacy whatsoever in any Company content.

Company may also make and preserve copies of all Company content, in Company's sole discretion, for a period of time after those copies are created and may delete those copies from time to time without notice. In addition, Company may obtain and disclose copies of any Company content for litigation, investigations, and as otherwise required by law.

By signing this policy and/or the handbook acknowledgment, you understand and consent to Company's monitoring, intercepting, reviewing, copying, disclosing, and remotely wiping all Company content, in Company's sole discretion. You also agree that the use of any device for Company's business or on behalf of Company is at your own risk and Company will not be responsible for any losses, damages, or liability arising out of the use of any device for Company's business or on behalf of Company under this policy, including any loss, corruption, or use of any content or loss of access to or use of any device, its software, or its functionality.

5.0 SECURITY REQUIREMENTS-GENERAL

All devices used for Company's business or on behalf of Company must be registered with and authorized by the Information Technology Department.

To protect Company's confidential business information from being lost or becoming public, you must immediately report any device used for Company's business or on behalf of Company that is lost, stolen, accessed by unauthorized persons, or otherwise compromised so Company can assess the risk and, if necessary, remotely wipe all Company content, in Company's sole discretion. You must also promptly provide Company with access to the device when requested or required for Company's legitimate business purposes, including in the event of any security incident or investigation.

Company's Acceptable Use Policy applies to all uses of your device for Company's business or on behalf of Company. To the extent Company's Acceptable Use Policy does not address the issues below, you must:

1. Consent to Company's efforts to manage the device and secure its data, including installation of Mobile Phone Management (MDM) software or other required software and providing Company with any necessary passwords or other means of accessing the device. This MDM software will store all company related information including calendars, emails and other applications in one area on the phone that is secured and allows Companies to manage those applications and data. Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup software that allows company-related data to be transferred to third parties. Due to security issues, personal phones may not be synchronized with other phones in the employee's homes.

2. Comply with Company's device configuration requirements.

3. Password protect the device through the use of strong passwords consistent with Company's current password policies and procedures.

4. Maintain the device's settings such that the device locks itself and requires a password if it is idle for five minutes.

5. Maintain the device's original operating system and keep it current with security patches and updates. Changes to the phones operating system intended to bypass software and security restraints commonly known as Jailbreaking or Rooting is not allowed on personal phones that are used for work related purposes.

6. Not alter the security settings of the device without Company's consent.

7. Not download or transfer work product or sensitive business content to your device, for example via email attachments. You must erase any such information that is inadvertently downloaded to your device.

8. Not back up or otherwise store Company content to cloud-based storage or services without Company's consent. Any such backups or other stored copies of Company content inadvertently created must be deleted immediately. To the extent you create backups or otherwise store Company content with Company's consent, you must provide Company with access to your cloud-based storage to access and review any such backups or other stored copies of Company content when requested or required for Company's legitimate business purposes, including in the event of any security incident or investigation.

9. Not transmit any Company information over an unsecured WiFi network.

10. Only Company-provided phones are eligible to be connected to the Company corporate network (personal devices may connect to the Company's guest network if there is a valid reason).

At all times, you must use your best efforts to physically secure the device against loss, theft, damage, or use by persons who have not been authorized to access the device by Company.

6.0 SECURITY REQUIREMENTS- INTERNATIONAL TRAVEL

To protect Company's confidential business information when employees travel internationally, it is critical that employees strictly adhere to Company's information and data security policies and procedures, as set forth in Company's Acceptable Use Policy. In addition to the requirements set forth in Company's Acceptable Use Policy, if you travel internationally, whether for business or leisure, with a personal electronic device with any Company content, you must:

1. Advise the Information Technology department of your international travel plans (personal or business if device will be accompanying you), including the dates of travel and the countries you intend to visit.

2. Follow any instructions of the Information Technology department regarding Company content on your personal electronic device.

3. Adhere to Company's policies and procedures for inspection and search of electronic devices by customs and border patrol officers, including immediately alerting officers that your device contains confidential business information, providing officers with your business card or company identification badge showing that you are a Company employee, and providing assistance to officers to access the device if it is encrypted or password protected according to Company policies and procedures.

7.0 APPROPRIATE USE

Company's policies prohibiting harassment, discrimination, and retaliation apply to the use of all devices under this policy. You may not use any device in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state, or local law.

Nonexempt employees using their own devices under this policy are not permitted to use their devices for work purposes during nonworking hours without prior written authorization from Company. This includes reviewing, sending and responding to e-mails, Microsoft Teams messages, text messages, responding to phone calls, or making phone calls. Supervisors of nonexempt employees must review the compensable time requirements under the Fair Labor Standards Act with Human Resources prior to nonexempt employees entering the BYOD program.

Any employee who discontinues use of their device under this policy or leaves Company's employ must allow Company to remove any Company content from their device and to disable any software or services provided by Company on their device.

Company prohibits employees from talking, texting, emailing, or otherwise using a mobile or other electronic device, regardless of who owns the device, while operating Company vehicles, machinery, or equipment, or while operating personal vehicles, machinery, or equipment for Company's business or on behalf of Company. Employees must also comply with any applicable federal, state, or local law restricting the use of mobile or other electronic devices while operating vehicles, machinery, or equipment. For their own health and safety and the health and safety of others, employees should not use their devices while operating vehicles, machinery, or equipment of any kind.

8.0 TECHNOLOGICAL SUPPORT

Company does not provide technological support for employee devices. By signing this policy and/or the handbook acknowledgment, you acknowledge that you alone are responsible for any repairs, maintenance, or replacement costs and services.

9.0 COSTS AND REIMBURSEMENTS

Company will reimburse employees a fixed amount for costs associated with their device usage for business purposes. Eligible employees will receive a reimbursement of $30 per month (subject to modification).

To be eligible for reimbursement, you must submit the attached form and a copy of your statement or bill substantiating your usage of the device for business purposes to Human Resources at the onset and again annually.

The Human Resources department will obtain the completed BYOD form from the employee annually and will submit the employee's names to finance and IT.

10.0 CONFIDENTIALITY AND PROPRIETARY RIGHTS

Company's confidential information and intellectual property, including trade secrets, are extremely valuable to Company. You must treat them accordingly and not jeopardize them through your use of your device. Disclosure of Company's confidential information to anyone outside Company and use of Company's intellectual property is subject to Company's Confidential Information Policy. Any work product created, stored, or maintained by you on your device is subject to Company's Confidential Information Policy and Intellectual Property Assignment Agreement.

11.0 CONSEQUENCES FOR FAILURE TO COMPLY

Employees who violate any provision of this policy are subject to discipline, up to and including termination of employment.

12.0 ADMINISTRATION OF THIS POLICY

Company expressly reserves the right to change, modify, or delete the provisions of this Bring Your Own Device to Work Policy without notice. In addition, if it is determined that there is insufficient value to the Company with respect to any employee in the BYOD program, that employee may be removed from the BYOD program unless and until circumstances change to provide sufficient value.

13.0 CONDUCT NOT PROHIBITED BY THIS POLICY

This policy is not intended to restrict communications or actions protected or required by state or federal law.

14.0 AUTHORITY

WRITTEN / REVISED BY	APPROVED BY	APPROVAL (Initials/Signature)	DATE

15.0 REVISION HISTORY

15.1 (Keeping track of the document changes by revision and content)

REV. #	REV. DATE	SCN No.	REVISED BY	CHANGES
1				Initial launch
2				
3		--		