Information Technology	Document No. ITP-003	Revision Level: 0	
Description: **Acceptable Use Policy**	**Issuer: Christopher Vanco**		
	Revised By: Christopher Vanco		**Revision Date:** 3/4/2021

Acceptable Use Policy

Last Update Status: Version 1.0 Updated 2/1/21 Sections: ALL

1. Overview

Except where otherwise specified, this policy applies to Zippo Manufacturing Company, W.R. Case & Sons Cutlery Company and Northern Lights Enterprises, Inc. including their subsidiaries listed in Appendices Section A. ("Companies").

Tech Services' intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Companies established culture of openness, trust, and integrity. Tech Services is committed to protecting Companies employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Companies. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Companies employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Companies. These rules are in place to protect the employee and Companies. Inappropriate use exposes

Companies to risks including virus attacks, compromise of network systems and services, and legal issues.

This Policy shall be in addition to other Company policies. It is the employee's responsibility to read and understand all Company policies located within the "Policy Manual" and employee handbook.

This Policy is not intended to preclude or dissuade employees from engaging in activities protected by Federal or State law, including the National Labor Relations Act.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Companies business or interact with internal networks and business systems, whether owned or leased by Companies, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Companies are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Companies policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Companies, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Companies. Except where otherwise specified within this policy.

4. Definitions and Terms

Technical Services or **Technical Services Team** is one of the teams within Companies Information Technology department and includes both the employees that are members of that team, and any third parties that they may designate to complete work on their behalf it may also

sometimes be referred to internally as Tech Services or Tech Svc. This team consists of various admins that manage and administrates Companies infrastructure such as the Network, Servers, Personal Computers, and other computing devices at Companies, and provides support via Companies Help Desk. The easiest way to contact the Technical Services Team is through the Help Desk by emailing Helpdesk@zippo.com.

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

Blogging
Honeypot
Honeynet
Proprietary Information
Spam

5. Policy

General Use and Ownership

1.1 Companies proprietary information stored on electronic and computing devices whether owned or leased by Companies, the employee or a third party, remains the sole property of Companies. You must ensure through legal or technical means that proprietary information is protected in accordance with all regulatory, statutory, and contractual obligations that apply to the data stored on the device and that the data is stored in accordance to Companies policies.

5.1.1 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Companies proprietary information.

5.1.2 You may access, use, or share Companies proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

5.1.3 In our US based employees, employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

5.1.4 For employees based in countries outside of the USA, personal use of Companies systems, and devices is prohibited to the extent allowed under local laws.

5.1.5 For security and network maintenance purposes, authorized individuals within Companies may monitor equipment, systems and network traffic at any time, to the extent allowed under local law.

5.1.6 Companies reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy except where prohibited under local law.

5.1.7 Companies reserves the right to audit networks and systems when necessary to conduct investigations into potential compromises or breaches of Companies systems, and in accordance with local law.

5.1.8 Upon request for the purpose of performing an audit, any access needed will be provided to members of Companies Tech Services team. This access may include:

5.1.8.1 User Level and/or system level access to any communication or communications device.

5.1.8.2 Access to information (electronic, hardcopy or otherwise) that may be produced, transmitted, or stored on Companies equipment or premises.

5.1.8.3 Access to work areas (offices, cubicles, storage areas, labs etc.)

5.1.8.4 Access to interactively monitor and log traffic on Companies networks.

5.1.9 Companies reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy to the extent allowed under local law.

2.2 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Companies authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Companies-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

5.2.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Companies.

5.2.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Companies or the end user does not have an active license is strictly prohibited.

5.2.3 Accessing data, a server or an account for any purpose other than conducting Companies business, even if you have authorized access, is prohibited.

5.2.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5.2.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5.2.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5.2.7 Using a Companies computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

5.2.8 Making fraudulent offers of products, items, or services originating from any Companies account.

5.2.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

5.2.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

5.2.11 Port scanning or security scanning is expressly prohibited unless prior notification to Tech Services is made.

5.2.12 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

5.2.13 Circumventing user authentication or security of any host, network or account.

5.2.14 Introducing honeypots, honeynets, or similar technology (as defined in the definition section of this document) on Companies network.

5.2.15 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

5.2.16 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5.2.17 Providing information about, or lists of, Companies employees to parties outside Companies.

5.2.18 Making configuration changes to Companies devices that bypass the built-in security measures of the operating system commonly known as Jailbreaking or rooting.

5.2.19 Any form of harassment via email, MS Teams, telephone, paging, or other means, whether through language, frequency, or size of messages

5.2.20 Installing unapproved applications or software on Companies devices.

3.3 Security and Proprietary Information

5.3.1 All mobile and computing devices that connect to Companies network must comply with the Remote Access Policy.

5.3.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

5.3.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

5.3.4 Postings by employees from a Companies email address to newsgroups is prohibited, unless posting is in the course of business as part of your job duties.

5.3.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware**.**

4.4 Password Policy

5.4.1 All of Companies Systems and Network Access must be configured to require a strong password or passphrase. Multi-Factor Authentication is strongly recommended.

5.4.2 All user-level and system-level passwords must conform to the following rules.

5.4.2.1 Minimum of 8 characters – We recommend at least 10.
5.4.2.2 Contain a mixture of letters numbers and special characters such as Z1pP0R0ckS!!!
5.4.2.3 May not use any of the last 24 passwords.
5.4.2.4 If possible, use a long pass phrase such as “1t’s-t1me-for-Vacat1on!!”.
5.4.2.5 Cannot contain your Username, System name, Company, or department names.
5.4.2.6 Patterns such as aaabbb, qwerty123, asdfjkl;, or 123321 Should be avoided.

5.4.3 Users must use a separate, unique password for each of their work-related accounts.

5.4.4 Users may not use any work-related passwords for their own, personal accounts.

5.4.5 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

5.4.6 Passwords should be changed at least every 30 days.

5.4.7 Password cracking or guessing may be performed on a periodic or random basis by the Tech Services Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.4.8 Passwords may be reset by utilizing the office 365 self-service password reset. Instructions can be found in the notification email that you receive when your password is about to expire, as well as this document. If you need assistance with resetting your password, please contact the Helpdesk.

5.4.9 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Companies information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

5.4.10 Passwords must not be inserted into email messages, Helpdesk Tickets, or other forms of electronic communication, nor revealed over the phone to anyone. Except in specific cases approved by Technical Service. Any such approval must occur prior to communication.

5.4.11 Passwords may be stored only in “password managers” authorized by the organization.

5.4.12 Do not use the "Remember Password" feature of applications (for example, web browsers).

5.4.13 Any user suspecting that his/her password may have been compromised must report the incident to the Helpdesk and change all passwords.

5.5 Password Reset instructions

If you are inside the Corporate Offices

Press the Ctrl + Alt + Delete keys simultaneously from your Windows workstation and select 'Change Password' from the available options.

If you are outside the Corporate Offices

Open a Web Browser and Navigate to the Office 365 Portal at https://portal.office.com/account

Enter your Username and Password and Click “Sign in”

On the left menu select "Security & privacy"

Select "Change your password"

On the next screen, Enter your “Current Password,” “New Password,” “Confirm new password,” and Click “submit”

If you are an Area Sales Manger

Connect to VPN and ensure you are connected

Press the Ctrl + Alt + Delete keys simultaneously from your Windows workstation and select 'Change Password' from the available options.

Insert current password along with your new password

Log off your computer and then back in with new password

Insert new password into Global Protect VPN when prompted

Connect to the VPN and ensure everything is working properly

6.6 Remote Access

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Companies’ policy, we must mitigate these external risks the best of our ability.

Employees and Contractors based in the United States of America may be authorized at Companies discretion to utilize personal devices to connect remotely via VPN. Employees based in other countries must use a Companies owned device to connect to the corporate network, and are prohibited from utilizing a personal device for work to the extent allowable by law.

5.6.1 It is the responsibility of Companies employees, contractors, vendors, and agents with remote access privileges to Companies' corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Companies.

5.6.2 When accessing the Companies network from a personal computer, Authorized Users are responsible for preventing access to any Companies computer resources or data by non-Authorized Users including other members of their household. Performance of illegal activities through the Companies network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

5.6.3 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For more information refer to the Password Policy section of this document and the Cryptographic Protections section of the Written Information Security Policy.

5.6.4 Authorized Users shall protect their login and password, even from family members.

5.6.5 While using a Companies-owned computer to remotely connect to Companies' corporate network, Authorized Users shall not be connected unsecured public networks, and must exercise caution when connecting to other secured networks such as hotel Wi-Fi etc., and must use Companies VPN in those scenarios.

5.6.6 Use of external resources to conduct Companies business must be approved in advance by Tech Services and the appropriate business unit manager.

5.6.7 All hosts that are connected to Companies internal networks via remote access technologies must use the most up-to-date anti-virus software, such as Microsoft Defender, this includes personal computers.

5.6.8 It is Companies policy that no device on which security controls have been intentionally subverted by the end user, such as a "jail broken" or "rooted" operating system be connected to Companies networks or systems.

5.6.9 **Any device connecting to Companies systems and/or network remote, or otherwise must meet the following requirements.**

5.6.9.1 Operating systems must be currently under support by the manufacturer and must not be considered end of life. Generally, this includes the last 2 major releases such as Windows 8 and Windows 10, or Mac OS X Catalina and Mojave. Refer to the manufacturer's websites for more information.

5.6.9.2 All operating system and security patches must be installed and up to date.

5.6.9.3 Anti-virus must be installed and up to date, and if possible configured to not be able to be turned off.

5.6.9.4 Malware scans should be run at least once a month to ensure nothing is missed by the Anti-virus software. Companies recommends Malwarebytes.

5.6.9.5 Full disk encryption should be utilized if available on mobile devices. If you have questions regarding acceptable encryption software, please reach out to the Help Desk.

5.6.9.6 All devices must be protected by a password and the screen locked when not in use.

7.7 Software Installation

5.7.1 Employees may not install unapproved software on Companies computing devices operated within the Companies network.

5.7.2 Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk via a ticket or email.

5.7.3 Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.

5.7.4 If new software is needed to meet the requester's need, the request must go through Technical Services, prior to purchase of new software.

5.7.5 Technical Services will conduct a security review on any new software request, along with a functionality review to ensure that the functionality does not exist in an already approved and purchased software.

5.7.6 The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation or provide a package for self-guided installation.

8.8 Clean Desk

5.8.1 In order to protect sensitive information , employees are required to follow a 'clean desk' policy as specified below.

5.8.2 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

5.8.3 Computer workstations must be locked when workspace is unoccupied.

5.8.4 Computer workstations must be shut completely down at the end of the workday.

5.8.5 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

5.8.6 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

5.8.7 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

5.8.8 Laptops and other portable computing devices must be either locked with a locking cable, locked away in a drawer when not at your desk, or taken home at the end of the workday.

5.8.9 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in any location.

5.8.10 All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5.8.11 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins.

5.8.12 Whiteboards containing Restricted and/or Sensitive information should be erased.

5.8.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

9.9 Data Classification Policy and Governance Roles

All employees must be familiar with Companies Data Classification policy. This policy defines four categories into which all Companies data can be divided:

Public

Internal

Confidential

Restricted Use

Companies data that is classified as Public may be disclosed to any person regardless of their affiliation with Companies. All other Companies data is considered sensitive and must be protected appropriately. This document provides definitions for and examples of each of the four categories following NIST recommendations.

Other policies within Companies data protection standards specify the security controls that are required for each category of data.

The various units and departments at Companies have numerous types of documents and data. To the extent that documents or data types are not explicitly addressed within this policy, each business unit or department should classify its data by considering the potential harm to individuals or Companies in the event of unintended disclosure, modification, or loss. Business units, or their data custodians may assist with the classification process and coordinate with the Technical Services Team to achieve consistency across Companies environments.

5.9.1 All data will be classified into one of four categories, Restricted, Confidential, Internal Use and Public as defined in this document.

5.9.2 When more than one category may apply the more restrictive category will be used.

5.9.3 The data owner will be responsible for the initial classification of the data.

5.9.4 Data classification will be reviewed upon modification, or movement of data.

5.9.5 Labels will be placed upon data where possible to ensure that the classification is known.

5.9.6 Governance Roles

5.9.6.1 There are 4 roles in Companies Data protection plan. Each of these roles have their own responsibilities for keeping Companies data secure and preventing data loss.

5.9.6.2 Data Owner

Data Owners are senior level employees with significant responsibility for a business unit or operational area that uses a system or application and/or creates or maintains data.

Major Responsibilities:

- Manage, protect, and ensure the integrity and usefulness of Companies Data.
- Identifies the sensitivity and critically of the data. Ensures that the appropriate practices are in place so that the data is secure, accurate and that employees are trained to maintain data quality.
- Ensure proper planning and governance needs are met.
- Works closely with Technical Services, legal, compliance and other senior level employees to ensure that the appropriate resources (staff, technical infrastructure, training etc.) are in place and dedicated to prioritizing data needs and setting/enforcing policies related to data management and use.
- Ensure proper policies are in place to remain in compliance with laws and contractual obligations related to data governance.
- Works closely with Technical Services, legal, compliance and other senior level employees to ensure that all Companies data protection policies are in place and meeting or exceeding contractual and legal obligations.
- Serves as an escalation point for issues related to data governance.
- Designates Data Stewards.
    - Data Owners may elect to also hold the role of Data Steward.

5.9.6.3 Data Steward

Data Stewards have oversight responsibility for a subset of Companies data. The steward is typically a functional user within an operational area who is deemed an expert regarding data managed by that area.

Major Responsibilities:

- Implement data standards.
    - Ensure that employees who maintain data are trained to follow standards.
- Monitor Data Quality

- Works with technical and operational employees to create and maintain processes for identifying data entry errors and correcting the data to meet Companies standards. Reports any issues that may require a larger action to the Data Owner.

- Handle inquiries about data
  - Receive and respond to any inquiries related to data that originates from the area that they oversee such as questions regarding access, standardization, organization, definition, usage etc.
- Authorize access requests.
  - Authorizes or denies requests for access to data that originates from the area that they oversee.

5.9.6.4 Data Custodian

Data custodians are a system administrator or other technical professional who are responsible for some aspect of the management and operation of any of the systems that create, modify, store, transmit or destroy Companies data.

Major Responsibilities:

- Provide a secure infrastructure
  - This includes but is not limited to physical security, backup and recovery processes, and secure storage and transmission of the data.
- Implement Data access policies
  - Grant access privileges to authorized users, documenting those with access and controlling level of access to ensure that individuals only have access to data for which they have been authorized and that access is removed in a timely fashion when no longer needed.
- Ensure System availability and performance

- This includes but is not limited to patching, configuration, upgrading hardware and software and ensuring that response times meet the need of the business.

- Participate in setting data governance priorities
  - Provide technical details on systems and staffing requirements related to data governance initiatives.

5.9.6.5 Data User

Data Users are individuals who have access to company data as part of their assigned duties.

Major responsibilities:

- Attending training and following Companies policies related to data management and governance.
- Reporting concerns related to data management and protection
  - Conveying appropriate concerns or observations to Companies management regarding weakness in data protection, failure to follow data management policies or specific issues of quality or integrity of Companies data.

5.9.7 Classification Levels

5.9.7.1 Public data is information that may be disclosed to any person or persons regardless of their affiliation with Companies. The Public classification is not limited to data that is intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect the original (source) document from unauthorized modification, Public data may be shared with a broad audience both within and outside of Companies and no steps need to be taken to prevent its distribution.

Examples of public data include press releases, advertisement material or directory information (not subject to other regulations).

5.9.7.2 Internal data is information that is potentially sensitive and not intended to be shared with the public. Internal data generally should not be disclosed outside of Companies without the permission of the data owner or creator.

It is the responsibility of the data owner to designate information as internal where appropriate. If you have questions about whether information is internal or how to treat internal data you should talk with your manager.

Examples of internal data include: some memos, emails, and meeting minutes, contact lists that contain information that is not publicly available or policy and procedural documentation that should remain private.

5.9.7.3 Confidential data is information that if made available to unauthorized parties may adversely affect individuals or Companies. This classification also includes data that Companies is required to keep confidential under a confidentiality agreement with a third party such as a vendor or by law. This information should be protected against unauthorized disclosure or modification. Confidential data should only be used when necessary for business purposes and should be protected both when in use and at rest.

The use of Confidential data must adhere to Companies' Confidential Information Policy.

Examples of Confidential data include trade secrets, personal data not covered under Restricted Use data, vendor numbers and financial data.

5.9.7.4 Restricted Use data is any data that Companies has a contractual, legal or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of data would require Companies to inform the affected individual, company, country or authorities. In some cases, modification of the data would require informing the affected individual.

5.9.8 Companies obligations will depend on the data and relevant contract, laws or regulations. Companies policy provides a baseline for all Restricted Use data. More stringent requirements exist for some types of Restricted Use data. Individuals as well as data owners and data custodians must ensure they meet all the requirements of their data type.

5.9.9 Examples of data with more stringent requirements include but are not limited to credit card data covered by PCI-DSS, Personal data covered by GDPR, Data controlled by U.S. Export Control Law, or health information covered by HIPAA.

10.10 Restricted Use Data Minimum Security Standard

This policy defines the minimum-security standards required for any data stored on, accessed by, or transferred via Electronic device, or cloud service classified as Restricted Use at Companies. This policy also applies to physical document containing information classified as Restricted Use at Companies per Companies 'Data Classification Policy'. Companies provides a minimum-security standard and all Data Owners and Data Stewards as defined in this policy are responsible for ensuring that their data is created, stored, transmitted and destroyed in accordance to any regulatory, compliance, or legal requirements beyond this policy.

This policy covers all computers and communication devices owned or operated by Companies. This policy also covers any computer, communication devices, cloud service or physical document that contains Companies data that has been classified as Restricted Use data. Companies recognizes that some Restricted Use data may require more stringent controls due to legal, regulatory, or contractual compliance requirements. In those cases, the requirements of the legal, regulatory, or contract take precedence over this policy.

5.10.1 Data Storage

5.10.1.1 All electronic Restricted Use Data must be stored on a server centrally managed by Companies Information Technology team, or in an environment that is under strict legal contracts with Companies that meet this policy and not on a workstation, laptop, portable storage device or locally managed server. Exceptions to this rule must be approved and documented by the Technical Services team.

5.10.1.2 All Restricted Use Data must be encrypted by an approved encryption technology.

5.10.1.3 All Physical documents containing Restricted Use data will be stored in a locked filing cabinet, within a locked room where access is monitored.

5.10.1.4 All backup media containing Restricted Use data must be encrypted by an approved encryption method as defined in the Written Information Security Policy.

5.10.1.5 All physical backup media containing Restricted Use data must be secured in a locked vault where access can be monitored and audited.

5.10.1.6 All Devices and systems storing Restricted Use data will be inventoried on a quarterly basis, or more often if there is reason to believe that the data has been compromised.

5.10.1.7 Data inventories as required in Section 1.6 will be the responsibility of the Data Steward or Data Owner as defined in this policy.

5.10.2 Data Access

5.10.2.1 Access controls to Companies Restricted Use data must be documented.

5.10.2.2 Companies Restricted Use data must have a designated Data Owner who authorizes such access.

5.10.2.3 Access to Companies Restricted Use will only be granted to individuals that have a documented business need and require access to do their job.

5.10.2.4 Access to Companies Restricted Use data will be monitored through access logs.

5.10.2.5 Access to Companies Restricted Use data is only permitted using a Companies-owned device. No personal devices can access Companies Restricted

Use Data. Company devices accessing Restricted Use Data must be up-to-date and meet the applicable Company device standards.

5.10.3 Data Transmission

5.10.3.1 All Restricted Use Data must be encrypted by an approved encryption method while in transit.

5.10.3.2 No Restricted Data may be transferred "in the clear".

5.10.3.3 Encryption keys will never be transmitted in the same communication as the encrypted data.

5.10.4 Release of Information

5.10.4.1 Restricted Use data may only be released in accordance with the laws governing the use of the data and must be approved by the Data Steward or Data Owner as defined in this policy.

5.10.5 Confidentiality

5.10.5.1 Data Owners who authorize access to Companies Confidential or Restricted Use data should ensure that those with access sign a Confidentiality or Non-Disclosure agreement or are otherwise bound to confidentiality obligations. All authorized users are also required to successfully complete Companies training regarding Confidential and Restricted Use data.

5.10.5.2 Media Destruction

5.10.5.3 Media containing Restricted Use data should be securely destroyed when removed from service and a Certificate of Destruction must be obtained and recorded by the Technical Services team.

5.10.6 Special Statements

The following statements are specific to various restricted information types.

5.10.6.1 GDPR

5.10.6.1.1 Data governed by GDPR must comply with all the requirements of GDPR including any not covered by this policy.

5.10.6.1.2 Companies maintains a separate GDPR policy in conjunction with this policy.

5.10.6.1.3 If you have a question regarding the storage, access, use or transmit of GDPR data contact the Technical Services Team. For a copy of the GDPR protection policy please contact Technical Services.

5.10.6.2 PCI-DSS

5.10.6.2.1 Data governed by PCI-DSS must comply with all the requirements of PCI-DSS including any not covered by this policy.

5.10.6.2.2 When possible PCI-DSS information should not be stored on Companies systems. Tokenization or other technologies should be used instead.

5.10.6.2.3 Data Stewards and Data Owners of PCI-DSS data are responsible to ensure that all regulatory requirements of the data are met.

5.10.6.2.4 If you have a question regarding the creation, storage, access, use or transmit of PCI-DSS contact the Technical Services Team.

5.10.6.3 HIPAA

5.10.6.3.1 Data governed by HIPAA must comply with all the requirements of HIPAA including any not covered by this policy.

5.10.6.3.2 Companies maintains a separate HIPAA policy in conjunction with this policy.

5.10.6.3.3 If you have a question regarding the creation, storage, access, use or transmit of HIPAA data contact the Technical Services Team. For a copy of the HIPAA policy please contact HR.

5.10.6.3.4 CTPAT

5.10.6.3.5 Data governed by CTPAT must comply with all the requirements of CTPAT including any not covered by this policy.

5.10.6.3.6 Data Stewards and Data Owners of CTPAT data are responsible to ensure that all regulatory requirements of the data are met.

5.10.6.3.7 If you have a question regarding the creation, storage, access, use or transmit of CTPAT contact the Technical Services Team.

5.10.7 Resolving Conflicts between this Policy and Other Policies and Regulations

5.10.7.1 Some data may be subject to specific protection requirements under a contract or according to a law or regulation not described here. In those circumstances, the most restrictive protection requirements should apply.

5.10.7.2 Data Stewards and Data Owners are responsible for ensuring that their data is created, stored, accessed, transmitted and destroyed in compliance with all regulatory or legal requirements for their data.

5.10.7.3 Data Stewards and Data Owners may reach out to Technical Services, and Companies legal team for assistance in complying with legal requirements and regulations.

11.11 Email and Communication Activities

5.11.1 When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

5.11.2 Email and/or Microsoft Teams shall be an employee's primary method for communicating an electronic message. Any Company record shall be made by email or by Microsoft Teams correspondence. Other forms of electronic communication such as text messaging, third party apps such as Messenger, WeChat, etc. will not be

considered appropriate formats for important information or Company records. Text messaging and unapproved third-party apps may be used for non-critical information such as making meeting arrangements or alerting employees to check their email or Microsoft Teams application for a message.

5.11.3 Companies email and/or Microsoft Teams account should be used primarily for Companies business-related purposes; Employees based in the USA of Zippo MFG, WR Case and Northern Lights Candles are permitted to use Companies communication technologies for personal communication on a limited basis, but non-Companies related commercial uses are prohibited.

5.11.4 Users not based in the USA are strictly prohibited from using any company communications technologies including email and Microsoft Teams for personal use.

5.11.5 Users are prohibited from sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) unless as part of an approved marketing campaign.

5.11.6 Users are prohibited from unauthorized use, or forging, of email header information.

5.11.7 Users are prohibited from creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5.11.8 Employees are prohibited from the use of unsolicited email originating from within Companies networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Companies or connected via Companies network.

5.11.9 All use of email and/or Microsoft Teams must be consistent with Companies policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

5.11.10 All Companies data contained within an email and/or Microsoft Teams message or an attachment must be secured according to all relevant data standards that apply to

the data. Examples include, but are not limited to Companies Confidential information policy, GDPR, Data retention laws etc.

5.11.11 Email and/or Microsoft Teams should be retained only if it qualifies as a Companies business record. Email and/or Microsoft Teams is a Companies business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email and/or Microsoft Teams.

5.11.12 Email and/or Microsoft Teams that is identified as a Companies business record shall be retained according to Companies Record Retention Schedule.

5.11.13 Companies email, Microsoft Teams or other communications systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any email and/or Microsoft Teams message with this content from any Companies employee should report the matter to their supervisor immediately.

5.11.14 Users are prohibited from automatically forwarding Companies email and/or Microsoft Teams messages to a unapproved third-party email and/or Microsoft Teams system. Individual messages which are forwarded by the user must not contain Companies confidential or above information.

5.11.15 Users are prohibited from using unapproved third-party email and/or Microsoft Teams systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Companies business, to create or memorialize any binding transactions, or to store or retain email and/or Microsoft Teams on behalf of Companies. Such communications and transactions should be conducted through proper channels using Companies-approved documentation.

5.11.16 Companies employees shall have no expectation of privacy in anything they store, send or receive on the company's email and/or Microsoft Teams system. Companies may monitor messages on any Company device or System, with or without prior notice. Employees should have no expectation of privacy in anything stored, sent or received on the Companies email or other System(s) to the extent provided by law. Companies is not obliged to monitor email and/or Microsoft Teams messages.

12.12 Blogging and Social Media

For purposes of this Policy, "social media" refers to websites, applications or similar systems comprised of electronic information where employees create or maintain online communities and profiles for the purpose of sharing and exchanging information and other content such as Facebook, Instagram, Pinterest, Twitter, YouTube and LinkedIn. The Company's policies and expectations for employees will apply to all use of social media.

5.12.1 Blogging by employees and engaging in other social media activities, whether using Companies property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Companies systems to engage in blogging and other social media activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Companies policy, is not detrimental to Companies best interests, and does not interfere with an employee's regular work duties. Blogging and other social media activities from Companies systems is also subject to monitoring.

5.12.2 Companies Data Classification Policy also applies to blogging other social media activities. As such, Employees are prohibited from revealing any of Companies confidential or proprietary information, trade secrets or any other material classified as Internal, Confidential, or Restricted Use when engaged in blogging other social media activities.

5.12.3 Employees shall not engage in any blogging other social media activities that may harm or tarnish the image, reputation and/or goodwill of Companies and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging

in any conduct prohibited by Companies Non-Discrimination and Anti-Harassment policies.

5.12.4 Employees may also not attribute personal statements, opinions or beliefs to Companies when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Companies. Employees assume any and all risk associated with blogging.

5.12.5 If an employee is required to use social media or blog as part of their job duties for the Company's marketing, public relations, recruitment, corporate communications or other business purposes, the Company owns all social media accounts, blogs or similar electronic information created or otherwise developed in the course of employees' employment or otherwise upon the request of the Company including any and all log-in information, passwords and content associated with each account, such as followers and contacts established on such accounts. The Company owns all such information and content regardless of the employee that opens the account or uses it and will retain all such information and content regardless of separation of any employee from employment with the Company. If job duties require an employee to speak on behalf of the Company in a social media environment, the employee must seek approval for such communication from the Marketing Communications Manager before any communication on behalf of the Company is posted.

5.12.6 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Companies trademarks, logos and any other of Companies intellectual property may also not be used in connection with any blogging activity.

6. Policy Compliance

1.1 Compliance Measurement

The Tech Services team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, automated and/or random checks and monitoring and feedback to the policy owner.

2.2 Exceptions

Any exception to the policy must be approved by the Tech Services team in advance.

3.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Appendices

Section A

Applicable Companies and subsidiaries

The following list contains company legal entities that these policies apply to.

- ZIPPO MANUFACTURING COMPANY (US)
- W.R. CASE & SONS CUTLERY CO. (US)
- ZIPPO UK, LTD. (UK)
- NORTHERN LIGHTS ENTERPRISES, INC. (US)

- ZIPPO S.A.S. (France)
- ZIPPO GmbH (Germany)
- ZippoLighters India Private Ltd (India)

Non-Applicable subsidiaries

The following list contains company legal entities that maintain their own policies wholly separate from the IT policies that apply to the rest of the company.

- ZIPPO ASIA, LTD. (Hong Kong)
- CLASSIC ZIPPO (BEIJING) COMMERCIAL CO., LTD. (china)
- ZIPPO CHINA OUTDOOR PRODUCTS CO., LTD. (China)

8. Related Standards, Policies and Processes

- Written Information Security Policy
- Confidential Information Policy
- Non-discrimination and Anti-Harassment Policy

9. Document Control Information

1.1 Approval Authority

Written / Revised By	Approved By	Approval (Initials/Signature)	Date
Christopher Vanco	Manager of Technical Services	Allen Robbins	3/4/2021
	Chief Financial Officer	Don Hall	3/5/2021

2.2 Revision History

Rev. #	Rev. Date	SCN No.	Revised By	Changes
0	3/4/2021	21-001	Christopher Vanco	Ownership Changed to IT, Policy re-written and re-released as new policy