Information Technology	Document No. ITP-001	Revision Level: 0	
Description: **Written Information Security Policy**	**Issuer: Christopher Vanco**		
	Revised By: Christopher Vanco		**Revision Date:** 3/4/2021

Written Information Security Policy

1 Overview and Purpose

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").

Companies written information security policy (“WISP”) is intended as a set of comprehensive guidelines and policies designated to safeguard all confidential and restricted use data maintained at Companies and to comply with applicable laws, regulations, and contractual obligations and covenants.
The WISP was implemented to comply with the various regulations that Companies data is subject to including, but not limited to PCI DSS, CTPAT, GDPR, HIPAA and any other regulations including state and local laws and regulations.
Companies is committed to protecting all sensitive data that it maintains and has implemented several policies to protect such information. The WISP should be read in conjunction with these policies that are referenced or linked throughout this document along with Companies “Acceptable Use Policy” and its’ associated policies.

2 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.

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.

3 Exceptions

While every exception to a standard potentially weakens protection mechanisms for Companies systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

Any exception to this policy or its associated policies, standards or procedures must be formally approved by Technical Services and documented, unless otherwise specified within the policy.

4 Conflicts

4.1 If two or more policies apply to the same system, data, process, or procedure and conflict with each other the most restrictive protection requirements should apply.

5. 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 Svs. 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.

least functionality is defined as only installing the software and services necessary to perform the business function that a system is intended for. It may also require the removal of unnecessary software or services installed by the manufacturer and blocking unnecessary network access.

Devices, Equipment, Electronic Devices, and Computer Equipment are all terms used to describe any device capable of storing, creating, transmitting, or modifying Companies data. This includes, but isn't limited to : Laptops, desktops, mobile phones, servers, routers, firewalls, switches, USB drives, disks, hard drives, etc.

Visitor is any individual on Companies premises that is not an employee, contractor, consultant, or other individual that Companies has authorized to access the facility on a regular basis.

6 Policy

6.1 Policy Reviews and Updates

6.1.1 This policy along with any associated policies, standards, procedures and guidelines will be reviewed and updated annually, or more often if deemed necessary due to a change in requirements, security posture or if the need arises as warranted by the business or Information Technology.

6.1.2 Updates to the WISP or associated policies, standards, procedures and guidelines will be announced to employees via management updates or email announcements. Changes will be noted in the Revision History located at the end of a policy, to highlight the pertinent changes from the previously published version.

6.2 Asset Tracking

6.2.1 Companies will maintain a record of all applicable electronic devices owned by companies including serial numbers and which employee the asset is assigned.

6.2.2 All data on an asset will be destroyed prior to redeployment to a new employee.

6.2.3 Technical Services will securely store all electronic devices until deployment or destruction.

6.2.4 The following asset classes are subject to tracking:

- Desktop workstations
- Laptop computers
- Tablet computers
- Printers, copiers, fax machines, scanners
- Handheld computer devices
- Barcode Scanners
- Servers
- Network appliances (e.g. firewalls, routers, switches, access points)
- PBX and Voip equipment
- IP enabled video and security devices
- Mobile Phones
- Memory devices

6.2.5 Asset Value

6.2.5.1 Assets which cost less than $100 may be excluded from tracking including computer components such as smaller peripheral devices, headsets, keyboards and mice as long as the component is not capable of storing any data.

6.2.5.2 All assets which store data regardless of cost will be tracked.

6.2.6 Tracked Information

6.2.6.1 The following is the minimal information that will be recorded for a tracked asset and retained.

- Date purchased.
- Cost
- Location
- Make, model, and description.

- Serial number
- Employee assigned.
- Department assigned.

6.2.6.2 Prior to repurposing an asset, all data on the asset will be destroyed, and the tracking database will be updated with the new employee assigned and department information.

6.2.6.3 Prior to deployment Technical Services shall enter the assets information into their tracking database

6.3 Asset Disposal

6.3.1 When devices have reached the end of their useful life they should be sent to the Technical Services Team for proper disposal.

6.3.2 No device may be sold to any individual other than though the process identified in this document.

6.3.3 No electronic devices should be disposed via skips, dumps, landfills etc.

6.3.4 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

6.3.5 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

6.3.6 The Technical Service Team will dispose of the device through an approved electronics recycling vendor.

6.3.7 The Technical Services team will inventory all devices being disposed of and maintain a record of all storage media (hard drives, backup tapes, disks, USB drives etc.) and the date the recycling vendor took possession.

6.3.8 Approved recycling vendors must provide a Certificate of Destruction (C.O.D) for all data storage devices stating that the media and associated was destroyed per DOD standards either by physically shredding the storage device or other pre-approved means.

6.3.9 Upon receipt of the C.O.D Technical Services will compare the serial numbers listed on the C.O.D to their inventory record to ensure all equipment was properly disposed of.

6.3.10 Technical Services will retain a record of the C.O.D for a period of 7 years.

6.3.11 If Companies determines that it wishes to offer used devices for sale to employees Technical Services will destroy all data to DOD standards prior to sale and keep records of the transfer of ownership for 7 years, including the dates data was destroyed and the device was transferred to the employee along with the employees' name.

6.4 Business Continuity and Disaster Recovery

6.4.1 Companies will maintain current Business Continuity and Disaster Recovery plans

6.5 Change Control

6.5.1 Companies will track changes to key production business systems through a change control process.

6.5.2 This process will require a change request to be submitted and approved before any configuration or application change to key business systems in the production environment.

6.5.3 Companies will track change requests and approvals throughout its change control process.

6.6 Configuration Management and Secure Engineering

6.6.1 Companies shall follow the concept of "least functionality" for its technology endpoints (any electronic device owned by Companies that connects to Companies systems or network) and proactively govern security mechanisms to keep its technology assets secure from evolving threats.

6.6.2 Technical services shall remove all applications not required by the operating system, or by approved business applications from endpoints prior to deploying them.

6.6.3 All Technology assets shall be hardened according to the appropriate hardening policies.

6.6.4 All vendor supplied default passwords will be changed prior to installing any device or system on the network including, but not limited to Software accounts, Network devices and wireless access points, Operating system passwords, device specific passwords, SNMP community strings etc.

6.6.5 Following the concept of "least privilege" no end user account shall have admin access to their device. Any exceptions to this policy will require business justification and require approval by Technical Services.

6.6.6 Companies configurations shall follow a "fail secure" methodology.

6.6.6.1 Any technology at Companies which controls access to Companies systems or data will be engineered to close access if the technology fails.

6.6.7 Technical Services will maintain a diagram of network flows.

6.6.7.1 A separate diagram will be maintained for any network connections to a cardholder environment.

6.6.7.1.1 Cardholder data flows will also be diagramed by the data steward or data custodian with the help of Technical Services, and those diagrams maintained.

6.6.8 Changes to Companies Firewalls and Network Router configuration must be approved by the head of Technical Services.

6.6.9 Technical services will maintain documentation of the business justification and approval for all services, protocols, and ports allowed through Companies firewalls.

6.6.9.1 For any required service, protocol, daemon etc., that is insecure Technical Services will implement additional security features as possible to mitigate the risk.

6.6.10 Technical Services will maintain, and inventory of all system components considered in scope for PCI DSS

6.6.11 All non-console administration access will be encrypted using strong cryptography as defined in Section 5.12 of this document.

6.6.12 All Systems commonly affected by malicious software will have anti-virus installed (particularly servers and personal computers) and configured in a manner which prevents it from being disabled, for systems not considered to be commonly affected periodic evaluations will be performed to identify and evaluate threats.

6.7 Network Hardening

6.7.1 Network devices will be configured based on Companies Network hardening standards. These Standards will include the following minimum hardening requirements.

6.7.2 All devices

6.7.2.1 Devices should be configured on a development network prior to being put into production if possible.

6.7.2.2 Install latest tested patches and updates.

6.7.2.3 Change default passwords.

6.7.2.4 Change default configuration settings (default SSIDs, vlans, administration passwords etc)

6.7.2.5 Disable unused management interfaces.

6.7.2.6 Enable logging and monitoring.

6.7.2.7 Institute a session timeout.

6.7.2.8 Disable unused ports.

6.7.2.9 Use a synchronized secured time source.

6.7.3 Firewalls

6.7.3.1 Ensure that latest signatures are installed for application-based firewall rules and that signatures are being downloaded from a trusted source.

6.7.3.2 Block spoofed, private and illegal addresses on public interface.

6.7.3.3 Ensure that the firewall rules have the readdressing option enabled such that internal IP addresses are not displayed to the external untrusted networks.

6.7.3.4 If the firewall is stateful, ensure packet filtering for UDP/TCP 53. IP packets for UDP 53 from the Internet are limited to authorized replies from the internal network. If the packet were not replying to a request from the internal DNS server, the firewall would deny it. The firewall is also denying IP packets for TCP 53 on the internal DNS server, besides those from authorized external secondary DNS servers, to prevent unauthorized zone transfers.

6.7.3.5 Ensure that there is a rule specifying that only traffic originating from IP's within the internal network be allowed. Traffic with IP's other than from the Internal network are to be dropped.

6.7.3.6 Ensure that any traffic originating from IP's other than from the internal network are logged.

6.7.3.7 Ensure that there is a deny rule for traffic destined to critical internal addresses from external sources. This rule is based on the organizational requirements, since some applications may require traffic via a web application to be routed via a DMZ.

6.7.3.8 Review the firewall access control lists to ensure that the appropriate traffic is routed to the appropriate segments at least twice a year or more often when significant changes to the networks are made.

6.7.4 Router Configuration

6.7.4.1 Router configuration files must be secured from unauthorized access.

6.7.4.2 Router configurations must be synchronized - for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).

6.7.5 Wireless Access Points

6.7.5.1 Ensure a proper Site Survey is performed

6.7.5.2 Ensure Strong Authentication and Encryption is required

6.7.5.3 Use the strongest encryption practical, 128 bits should be considered the minimum acceptable level.

6.7.5.4 Use AES with WPA2 if possible.

6.7.5.5 Select a mechanism that uses centralized authentication.

6.7.5.6 Select a mechanism that supports PKI certificates if possible.

6.7.5.7 Assume that WEP provides no real protection and only use as a last resort.

6.7.5.8 Avoid using authentication protocols that have been broken.

6.7.5.9 Use an Out-of-Band network or separate VLAN to handle management of the access points.

6.7.5.10 Do not broadcast the SSID where feasible.

6.7.5.11 Implement an IDS/IPS if possible.

6.7.5.12 Use Wireless client isolation on networks where there is no compelling business reason not to. Especially Guest networks

6.8 Server Hardening

6.8.1 Companies Servers will be configured based on Companies Server hardening standards. These Standards will include the following minimum hardening requirements.

6.8.2 All Servers

6.8.2.1 Devices should not be connected to the Companies network until fully configured and tested.

6.8.2.2 Install latest tested patches and updates.

6.8.2.3 Change Administrator or Root password

6.8.2.4 Disable Roles, Features, and Services that are not needed for the intended function.

6.8.2.5 Ensure file permissions for guest, everyone, and anonymous are removed.

6.8.2.6 Ensure only Administrators and specific users whose job requires it, can access the server remotely via RDP and/or SSH.

6.8.2.7 Install Antivirus software and configure appropriately. Ensure that configuration prevents users from disabling or turning off the Antivirus software.

6.8.2.8 Set system date / time to pull from the domain time servers.

6.8.2.9 For interactive sessions configure machine to lock after period of 10 minutes of inactivity or to log out the user if possible

6.8.2.10 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.

6.8.2.11 Disable AUTORUN.

6.8.2.12 Enable logging and monitoring based upon server function and Company standards.

6.8.3 Windows Servers

6.8.3.1 Ensure server is in the proper Active Directory OU and proper group policies apply.

6.8.3.2 Require Ctrl+Alt+Del for interactive logins.

6.8.3.3 Disable AUTORUN.

6.8.4 Linux Servers

6.8.4.1 Configure a password policy to match Companies Password Construction Guidelines

6.8.4.2 Remove or disable Telnet.

6.8.4.3 Disable SNMP daemon unless needed for the role of the server.

6.8.4.4 Ensure that permissions are set so that only Administrators with root permissions can edit sensitive system files and access sensitive binaries.

6.9 Workstation Hardening

6.9.1 Companies Workstations will be configured based on Companies Workstations hardening standards. These Standards will include the following minimum hardening requirements.

6.9.2 Install latest tested patches and updates.

6.9.3 Change Administrator or Root password

6.9.4 Ensure no users other than Technical Services and the Administrator are in the Administrators group. Users should not administrators on their workstation.

6.9.5 Disable services that are not needed for the intended function of the workstation.

6.9.6 Ensure file permissions for guest, everyone, and anonymous are removed where possible.

6.9.7 Uninstall all unnecessary software and applications.

6.9.8 Ensure only Administrators and specific users whose job requires it, can access the workstation remotely via RDP.

6.9.9 Install antivirus software and configure appropriately. Ensure configuration does not allow users to turn off or disable the antivirus software.

6.9.10 Set system date / time to pull from the domain time servers.

6.9.11 For interactive sessions configure machine to lock after period of 10 minutes of inactivity or to log out the user if possible

6.9.12 Enable logging and monitoring based on workstation role and company standards.

6.9.13 Ensure workstation is in the proper Active Directory OU and proper group policies apply.

6.9.14 Enable disk encryption on laptops and mobile devices if possible.

6.9.15 Require Ctrl+Alt+Del for interactive logins.

6.10 Continuous Monitoring

6.10.1 Continuous monitoring helps to ensure that Companies systems remain compliant with its policies. Companies utilizes a continuous monitoring policy for its key systems and network focused on real time monitoring and automated alerts.

6.10.2 Companies utilizes an "automated alerting first" approach to continuous monitoring.

6.10.3 Technical Services will conduct quarterly vulnerability scans of its DMZ and public systems.

6.10.4 Technical Services will augment the quarterly scans with additional scans when changes are made to the public or DMZ environments, or if they have reason to believe an additional scan is warranted.

- Where technology allows Technical Services shall configure alerting on the following for Servers and workstations:
- Installed patches.
- Missing patches
- New local user accounts
- Changes to existing configuration items
- Missing configuration items
- Vulnerabilities to the local systems
- Known threats.
- Malware
- Viruses

6.10.5 Where Companies technology allows Technical Services shall configure alerting on the following for network devices:

- Installed patches.
- Missing patches
- New local user accounts
- Changes to existing configuration items
- Missing configuration items
- Vulnerabilities to the local systems
- Known threats.
- Rogue access points

- Open ports

6.10.6 Companies recognizes that some systems may require additional scanning, alerting, and monitoring to comply with regulatory, legal and contractual obligations. Technical Services will implement scanning, monitoring and/or alerting procedures on such systems to ensure that the regulatory, legal or contractual obligations are met.

6.11 Statutory, Regulatory, & Contractual Compliance

6.11.1 Some of Companies systems and data may have statutory, regulatory, or contractual obligations and requirements above or beyond the scope of Companies published policies. It is the responsibility of the data owner or system owner to ensure that these obligations and requirements are met.

6.11.2 If the circumstance arises where this policy or any company policy does not meet a statutory, regulatory, or contractual requirement, the statutory, regulatory or contractual requirement shall take precedence over Companies policy.

6.12 Cryptographic Protections

6.12.1 Companies will encrypt sensitive data in transit and at rest using strong cryptography in accordance with the requirements set forth below.

6.12.2 **Algorithm Requirements**

6.12.2.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

6.12.2.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

6.12.2.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider RFC6090 to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

6.12.2.4 Hash Function Requirement

6.12.2.4.1 In general, Companies adheres to the NIST Policy on Hash Functions.

6.12.2.5 Key Agreement and Authentication

6.12.2.5.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

6.12.2.5.2 End points must be authenticated prior to the exchange or derivation of session keys.

6.12.2.5.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

6.12.2.5.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

6.12.2.5.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

6.12.2.6 Key Generation

6.12.2.6.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

6.12.2.6.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

6.13 Data Classification and Handling

6.13.1 It is the responsibility of every employee, consultant, and other designated individuals working for Companies or on Companies behalf to understand how to identify, and properly treat Companies information according to their role at Companies.

6.13.2 It is the Data Owners responsibility to ensure that all statutory, regulatory, and contractual requirements and obligations that apply to their data are met.

6.13.3 Companies information both electronic and physical, collectively referred to as “data” is classified into four categories.

6.13.3.1 **Public** – data that may be released to the public and has no negative impact for Companies, its affiliates or individuals associated with Companies.

6.13.3.2 **Internal** – data that is potentially sensitive and not intended to be shared with the public.

6.13.3.3 **Confidential** – data that if made available to unauthorized parties may adversely affect individuals, Companies' affiliates, or Companies.

6.13.3.4 **Restricted Use** – data that Companies has contractual, legal, or regulatory obligation to safeguard in the most stringent manner.

For more information on how to identify and treat Companies data refer to the Data Classification and Governance Roles section of Companies Acceptable Use Policy

6.14 Identification and Authentication

6.14.1 All users will have a unique ID for system access.

6.14.2 Companies adopts and utilizes the concept of "least privilege."

6.14.2.1 Users and Accounts will only receive the permissions and access necessary to complete the tasks associated with their role within Companies.

6.14.3 Technical Services will monitor for and disable and remove stale accounts.

6.14.4 Users will reset their password via self-service password reset when possible. If the Helpdesk is contacted to reset a user's password, the user's identity will be verified either by being face to face (physically or virtually) in the case that the user is known to the IT team member, or by contacting the requestor's manager to verify the employee is requesting the change prior to resetting the password.

6.14.5 All Accounts will be configured to lockout for a minimum of 30 minutes after no more than 6 failed login attempts. Some accounts may be more configured to be more restrictive.

6.14.6 All passwords must be set to expire every 60 days maximum; some accounts may be set to expire more often.

6.14.7 Multifactor authentication technologies will be utilized when possible.

6.14.8 Vendor accounts for accessing Companies systems will only be provisioned when required.

6.14.9 Vendor access to Companies systems will be terminated immediately upon completion of the work, or contract.

6.14.10 All Accounts will be provisioned and de-provisioned in accordance with the following requirements.

6.14.10.1.1 All requests for new user accounts will be generated by the HR department or hiring manager utilizing the new hire form.

6.14.10.1.2 All requests for new system or service accounts will be generated by system owners or application owners.

6.14.10.1.3 Technical services will work with the requester to determine the minimum rights required for the account.

6.14.10.1.4 All new passwords will be generated utilizing a random password generator and conform to Companies password policies.

6.14.10.1.5 All user accounts will be set to "user must change password on next logon" prior to the account being given to the user.

6.14.10.1.6 Account information will be verbally provided to the user's supervisor for user accounts, or the requester for system and service accounts.

6.14.10.2 **The account de-provisioning procedure will adhere to the following requirements.**

6.14.10.2.1 For all user accounts HR or the Manager will notify Technical services of a termination immediately.

6.14.10.2.2 Technical services will terminate all access to company resources disable the user account immediately.

6.14.10.2.3 Disabled accounts will be removed after a period of 1 year unless the employee is on litigation hold.

6.14.10.2.4 Technical services will monitor for stale service accounts.

6.14.10.2.5 Technical services will disable any system or service account that has not been accessed for 90 days.

6.14.10.2.6 Technical Services will delete stale accounts after 1 year.

6.15 Incident Response

6.15.1 All employees and contractors at Companies will be trained annually on the "Incident Response Plan" based on their role.

6.15.1.1 Employees who do not have direct responsibility within the incident response team as a member, executive or systems / data owner will be trained how to report cyber security events at Companies, by immediately reporting the event to the Helpdesk.

6.15.2 Cyber Security events at Companies will be investigated and handled according to companies' "Incident Response Plan".

6.15.3 Companies will partner with their internal legal team, along with outside legal teams as warranted to determine the best plans for communications including timing and content regarding a cyber security event.

6.16 Security Awareness Training

6.16.1 Companies will require Employees to complete quarterly Security Awareness Training.

6.16.1.1 Training will encompass Companies various security policies as applicable to the employee's role along with other privacy and information security topics.

6.16.1.2 Companies security awareness training will meet or exceed training requirements as stipulated by Companies statutory, regulatory, legal, and contractual obligations.

6.16.1.3 Companies will require additional training for privileged users.

6.17 Technology Development and acquisition

6.17.1 All technologies developed at Companies will be developed with security in mind. Application developers must ensure that their programs contain the following security precautions:

6.17.1.1 Companies will maintain a separation of development, testing and operational (production) environments.

6.17.1.2 Applications must support authentication of individual users, not groups.

6.17.1.3 Applications must not store passwords in clear text or any easily reversible form.

6.17.1.4 Applications must not transmit passwords in clear text over the network.

6.17.1.5 Applications must provide for a form of role management, such that one user can take over the functions of another without having to know the other's password.

6.17.1.6 Multi-Factor Authentication is highly recommended. Companies also recommends single sign on through Azure AD.

6.17.2 No employee shall provide Companies data to or enter a contract with a 3rd party technology provider without the express approval of Information Services following a security review.

6.17.3 No application or cloud service shall be purchased or installed on Companies Systems without prior approval by Information Services.

6.18 Third Party Management

6.18.1 Companies will require all third parties associated with Companies, including vendors, distributers, cloud services and other entities that may have access to companies' systems or data to annually provide proof that they maintain a security posture that meets companies' requirements based on the level of access to data and systems at Companies.

6.18.2 Prior to signing any agreement with a third party that will access Companies systems or data the vendor must complete Companies Vendor Due Diligence form, or provide other proof that meet all applicable compliance requirements for the data that they will have access to. Examples of other proof include valid PCI attestations, HIPPA certifications, ISO certifications, Soc2 etc.

6.18.2.1 Vendors that will have access to Companies restricted data will be sent the long version of Companies Vendor Due Diligence form.

6.18.2.2 Vendors that do not have access to Companies restricted data will be sent the short version of the Companies Vendor Due Diligence form.

6.18.2.3 The proof of compliance will be reviewed by IT Security and a record maintained in Companies SharePoint system.

6.18.2.4 Following the review by IT Security, any risks identified will be conveyed to the business so that they can make an informed decision on their vendor selection.

6.18.3 Vendor contracts must also be reviewed by the legal team prior to signing.

6.18.4 Companies will maintain a list of vendors and their proof of compliance in Companies SharePoint system.

6.18.5 Companies list of vendors will include information about which PCI DSS requirements are managed by each service provider.

6.18.6 Companies will also review each vendor that has access to Companies restricted data on an annual basis to ensure that they are remaining compliant.

6.18.6.1 Companies will utilize the same form and/or require the same proof of compliance for the annual audits as they do for new vendors as mentioned above.

6.18.6.2 Companies will keep a record of the audit in Companies SharePoint System.

6.19 Vulnerability, Patch Management and Risk Management

6.19.1 Updates and patches will be tested prior to installation where possible.

6.19.2 System Owners will be responsible for ensuring that all Companies' systems remain up to date with security patches. Critical Patches must be installed within 1 month of release.

6.19.2.1 Technical Services will ensure that all servers and workstations are using an operating system that is still supported by the manufacturer in that the manufacturer is still releasing security updates for that operating system.

6.19.2.2 Application Owners will ensure that all applications are up to date and have all security updates applied.

6.19.2.3 Business units within Companies will work with System Owners and Application owners to identify maintenance windows for all systems and applications at companies allowing patches and updates to be installed at least once a month.

6.19.2.4 Technical Services will monitor for zero-day vulnerabilities and patches and apply out of band patches as necessary to keep Companies data and systems secure.

6.19.2.5 Information Security will follow Companies Risk Management Policy to identify, assess, track and prioritize risks.

6.20 Physical Security

6.21 All Employees of large offices where employees are not known by sight will be issued security badges.

6.22 Employees of smaller offices where all employees are known by sight will be issued ID badges if travelling to a larger facility.

6.23 All Visitors to any of Companies facilities are required to enter through the reception area, sign in, and wear a visitor badge at all times.

6.24 All visitors must be accompanied by a Companies employee when on Companies property.

6.25 All sensitive areas (such as areas storing sensitive information) must be secured either through badge access, key card access, or physical lock and key, and access to these areas should be logged.

6.26 Upon termination the following actions will be taken:

6.26.1 Physical access to Companies sensitive areas will immediately be revoked

6.26.1.1 ID badges collected.

6.26.1.2 Physical keys collected.

6.26.1.3 Key cards disabled.

6.27 For more information on Companies physical security policies please see your employee handbook.

7 Appendices

7.1 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

- Acceptable Use Policy
- Confidential Information
- Incident Response Plan

9 Document Control Information

9.1 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

9.2 Revision History

Rev. #	Rev. Date	SCN No.	Revised By	Changes
0	3/4/2021	21-001	Christopher Vanco	Initial Release