1.0 PURPOSE

1.1 From time to time, certain employees may have access to written or electronic documents or similar materials containing information protected by law or Company policy. This information may include, for example, individuals' social security numbers, health information, financial information, or other protected information described below.

1.2 It is critical that employees follow certain procedures in order to keep this protected information secure, satisfy the Company's responsibilities, and comply with applicable law. A failure to do so could subject the employee and the Company to legal liability, and may subject the employee to discipline, up to and including termination. While several Company policies may govern matters at issue in this Policy, this Policy sets forth the minimum requirements that all employees must follow regarding these matters.

2.0 SCOPE & DEFINITIONS

2.1 This Policy governs employees of the "**Company**," which is Zippo Manufacturing Company, its subsidiaries (including W.R. Case & Sons Cutlery Company and Northern Lights Enterprises, Inc.) and any affiliates.

2.2 This Policy applies to a broad range of "documents." For the purposes of this Policy, a "document" is any written, electronic, or other material created, sent, received or maintained by the Company, including any paper, e-mail, computer file, instant message, voice message, video or audio recording or other material containing information. This Policy governs such documents when, for example, they are created, sent, received or maintained by the Company in physical files, on Company computers, laptops or mobile devices, on Company thumb drives or similar physical storage devices, on the Company's computer network or using the Company's internet access.

2.3 This Policy requires employees to take certain actions with respect to any "Protected Document." A Protected Document is a document that, due to either applicable law or Company policy, must be protected from view or use by certain persons, stored securely, kept confidential or subjected to similar controls. For example, a document will be a Protected Document under this Policy if it contains or otherwise shows:

2.3.1 Any social security number(s) or driver's license number(s) (which may be contained in, for example, an employee's personnel file);

2.3.2 Health information including, but not limited to, medical information, biometric information, and genetic information (which may be contained in, for example, medical examination records, disability benefits claim forms, notes from doctors, requests for Family and Medical Leave Act leave due to medical conditions or disabilities, certain workers' compensation documents, fitness-for-duty results, functional capacity assessments, return to work documents, records of an employee's an employee assistance program, results of drug or alcohol tests, health-related information about an employee's family members, insurance enrollment forms and any documentation about past or present health, medical condition or disabilities);

2.3.3 Attorney-client privileged information or confidential attorney work product (which may be contained in, for example, an email or memorandum from a Company internal or external attorney);

2.3.4 A person or entity's credit or financial information, including, for example, credit or debit card numbers, credit reports and other consumer credit information, bank account information and personal financial records (such as bankruptcy records);

2.3.5 Immigration-related information (which may be contained in, for example, Form I-9 paperwork and supporting documents or visa paperwork);

2.3.6 The Company's trade secrets or other confidential and proprietary business information;

2.3.7 Another person's e-mails, instant messages, or other written or electronic communications of that other person when they are viewed or used by a person who was not an intended recipient and who does not have a legitimate business need to view them (with the understanding that this does not negate or diminish any provision of the Company's Electronic Information and Acceptable Use Policy and related policies); and

2.3.8 Passwords, personal identification numbers, account numbers, or similar information that may allow a person to view or otherwise use any Protected Document or any individual's personal account of any type, either directly or when used in conjunction with other publicly available information (including any password or personal identification number to a person's personal e-mail account, bank account, or social media account).

2.4 There will be situations where a person may view or otherwise use a Protected Document in accordance with Company policy and applicable law, i.e., when a person is an "Authorized User." A person will be an Authorized User of a specific Protected Document only if the person is viewing and using the Protected Document:

2.4.1 In accordance with applicable law;

2.4.2 In accordance with all applicable Company rules, policies, and procedures; and

2.4.3 Only to the extent necessary to achieve a legitimate business purpose that arises from the employee's job duties.

2.5 A person will not be an Authorized User of a Protected Document and will not have a legitimate business need to view or use a Protected Document if that person is viewing or otherwise using that Protected Document for personal interest or some similar personal purpose. Accordingly, viewing or using a Protected Document for personal interest or some similar personal purpose is a violation of this Policy (subject to Section 3 below).

3.0 REQUIREMENTS

3.1 <u>Employees must ensure that Protected Documents are secured appropriately at all times.</u>

3.1.1 The required security will depend on the Protected Document at issue but, at a minimum, all Protected Documents must:

3.1.1.1 If created, maintained, or received electronically: Protected by a secured password or maintained in a similarly secured location (e.g. on a server or electronic folder that is only accessible to Authorized Users). (For the avoidance of doubt, emails that are Protected Documents are considered protected by a secured password since a password is required to open email programs and, similarly, a computer file will be considered protected by a secured password when it is maintained on a computer that itself has a secured password); and

3.1.1.2 If created, maintained, or received in physical form (e.g., in paper or on a thumb drive): Secured in an appropriate physical location that is protected by a lock.

3.1.2 No employee may allow a person to view or otherwise use a Protected Document unless the employee has confirmed that the other person is an Authorized User with respect to that Protected Document. Any new vendors, business partners or employees must be appropriately vetted in order to ensure that the person will abide by applicable laws and Company policies regarding Protected Documents before being treated as an Authorized User of any Protected Document.

3.1.3 It shall not be a violation of this Policy for an Authorized User to remove a Protected Document from a locked cabinet or room, or to view a Protected Document on a computer or other electronic device, only to the extent necessary for the Authorized User to satisfy a legitimate business need, and with the understanding that the Authorized User must secure the Protected Document as much as possible and otherwise comply with all applicable Company policies. For example, it shall not be a violation of this Policy for an authorized human resources official to remove a medical record from an employee's medical file when necessary to view that document to satisfy a legitimate business need, provided that the employee shields the document from third party view during the time it is being used and removes the document only as long as necessary to view or otherwise use the document.

3.1.4 If an employee is the Company's initial recipient, creator or custodian of a Protected Document, or if the employee otherwise receives a Protected Document that is not already secured in accordance with this Policy, that employee is responsible for ensuring that the Protected Document is secured appropriately as set forth in this Policy (and, depending on the situation, other employees also may be equally responsible for doing so). This is the case, for example, if an employee receives a Protected Document from:

3.1.4.1 A newly hired employee (who might provide, for example, her social security number, driver's license or similar information);

3.1.4.2 A customer (who might provide, for example, credit or debit card information);

3.1.4.3 A coworker who has not already secured the Protected Document as appropriate; or

3.1.4.4 A vendor or business partner (who might, for example, provide financial account information).

3.1.5 No employee may share any password that is used to secure any Protected Document, except with another Authorized User when approved by an authorized Company manager, unless circumstances dictate that the other Authorized User requires a separate account or username and password, in which case that should be created for that other Authorized User. All passwords must be appropriately complex, and reconfigured periodically, in a manner sufficient to prevent a third party from determining the password or otherwise in accordance with any instructions provided by an authorized Company manager. No employee may share any physical key or lock combination that allows another person to view or otherwise use any Protected Document unless that person also is an Authorized User for the Protected Document at issue.

3.1.6 Certain types of Protected Documents also will be subject to additional requirements. Although there are many situations where this will be the case, the following are examples:

3.1.6.1 Protected Documents containing health information must be maintained separately from an employee's general personnel file;

3.1.6.2 Form I-9s and supporting documents, as well as visas, should be maintained separately from an employee's general personnel file; and

3.1.6.3 If an employee is responsible for disposing of any Protected Document (in compliance with Company policy), the employee must do so in a way that does not allow the Protected Document to be viewed or used in a manner that would violate this Policy.

3.2 <u>Employees must help the Company prevent and address any violations by others regarding Protected Documents.</u>

3.2.1 In order to allow the Company to prevent violations and implement any necessary corrective steps in the event a violation does occur, an employee must notify the most appropriate Company manager (and any other Company employee who is required to receive notice pursuant to any Company policy or law) if the employee becomes aware of:

3.2.1.1 any violation of this Policy;

3.2.1.2 any fact or situation that could create a violation of this Policy in the future (e.g., any security threat or improperly vetted vendor);

3.2.1.3 any new source of a type of Protected Document (e.g., a new vendor that will begin providing a new type of Protected Document for which the Company does not have a designated secured location);

3.2.1.4 any fact or situation that, to the employee's knowledge, requires the Company to provide notice to a third party regarding a Protected Document; or

3.2.1.5 any person (including any Company employee) attempting to view or use any Protected Document when that person is not an Authorized User for that Protected Document.

3.2.2 Further, if an employee becomes aware that the Company is receiving, creating or maintaining any Protected Document but the Company has no legitimate business need to be doing so (even if the Company is securing that Protected Document as required), the employee should notify the most appropriate Company manager so that the Company can determine whether to stop receiving, creating or maintaining that Protected Document going forward. An employee must provide this notice if, for example, the employee becomes aware that social security numbers are being used as "identifiers" for any persons or that the Company is retaining a Protected Document long after any legitimate business need exists.

3.2.3 Employees must abide by all other applicable Company policies concerning the matters at issue in this Policy including, but not limited to, by refraining from downloading or installing any software in a manner that violates the Electronic Information and Acceptable Use Policy.

3.3 Other Important Considerations.

3.3.1 It is recommended that employees who may be Authorized Users review this Policy at least annually. Any employee who has a question regarding this Policy or a situation governed by this Policy should contact the Senior Vice President of Human Resources as soon as possible.

3.3.2 The matters at issue in this Policy also may be governed by other Company policies, including policies addressing specific types of Protected Documents. Nothing in this Policy should be interpreted to impose any restrictions that would be prohibited by applicable law, such as a prohibition on a person using information when the person has an affirmative legal right to do so even notwithstanding this Policy.

4.0 REFERENCES

4.1 Employee Handbook
4.2 Electronic Information and Acceptable Use Policy
4.3 Conflict of Interest Policy
4.4 Confidential Information Policy
4.5 Solicitations, Distributions and Postings of Materials Policy

5.0 APPROVAL AUTHORITY

WRITTEN / REVISED BY	APPROVED BY	APPROVAL (Initials/Signature)	DATE
Ed Hayden	**Bruce Gallagher**		
	Bunny Comilla		
	Beth Seals		

6.0 REVISION HISTORY

REV. #	REV. DATE	SCN No.	REVISED BY	CHANGES