**About Information Security:**

Objective of the Handbook: This Handbook was created to ensure that all Poetry Publishing employees understand and comply with the company's information security regulations, to ensure the safety of company and customer information. .

The importance of information security for Poetry Publishing: Information is a valuable asset of the company and information security is an important factor that helps ensure the trust and reputation of Poetry Publishing in the eyes of customers .

Company commitment to information security: Poetry Publishing is committed to complying with all information security regulations, ensuring the privacy and protection of customer and employee information.

**Privacy Policy:**

General regulations on information security: All Poetry Publishing employees must comply with the information security regulations and measures set forth in this Handbook and in related policies.

Basic principles to follow: The principle of least privilege, the principle of separation of duties, and the principle of multi-layer protection are the basic principles that every employee must comply with when working. with company information.

Division of responsibilities and roles in information security: Clearly describe the roles and responsibilities of each department and employee, including division of responsibilities for information security and reporting security incidents.

**Account and Password Management:**

Instructions on creating and managing secure passwords: Describes how to create strong and secure passwords, including the use of special characters, upper/lower case letters, and numbers.

Periodic password change policy: Clearly stipulate periodic password changes (for example, every three months) to ensure system security.

Grant access based on the principle of least privilege: Describes how to grant access so that users only have access to the information and resources they need to do their jobs.

*Instructions on creating and managing secure passwords:*

Describe how to create a strong and secure password: A strong password must be of sufficient length, at least 8 to 12 characters. To increase strength, it needs to contain at least one uppercase letter, one lowercase letter, one number, and one special character such as @, #, or %. For example, a strong password might be "Str0ngP@ssw0rd!".

Describe how to securely manage passwords: Encourage employees to use password management tools like LastPass or 1Password to store and manage their passwords. Do not share your password with others or store your password in a public place such as email or write it down on paper.

*Periodic password change policy:*

Rules for periodically changing passwords: All employees must change their passwords every three months. This helps ensure that passwords remain secure and cannot be misused if anything goes wrong. The system will automatically ask employees to change their password before it expires.

Instructions for employees to change passwords: When receiving a notice requesting a password change, employees need to change their password immediately. They should not reuse old passwords or passwords that have been used in the past.

*Grant access based on the principle of least privilege:*

Description of how to grant access rights: Grant access rights based on the principle of least privilege, which means granting only those rights necessary to perform each employee's specific job. For example, an editor only needs access to edit and publish content, not access to the company's account management system or database.

New access request process: Any new access request must be approved by the respective department's manager and confirmed as necessary for the user's work. This process ensures that access is granted only when absolutely necessary and does not pose a security risk to the system.

**Protecting Critical Data:**

Classify important information and define how to handle it: Guidance on how to classify critical, sensitive and public information, and prescribe how to handle and store it securely.

Guide to data and file encryption: Describes how to use encryption technology to protect data at rest and in transit, including file and email encryption.

*Categorize important information and clearly define how to handle it:*

Description of information classification: Poetry Publishing documents and information will be classified into three categories: Critical and sensitive information (such as customer account information and financial information), public information (such as information about announced products and projects), and internal information (such as internal company information). Each type of information will be marked and processed accordingly.

Regulations on how to handle and store them: Important and sensitive information will be strictly protected, accessed only by those with necessary access rights and stored in a system with measures in place. High security. Public information and internal information will be carefully managed and stored but with a more flexible level of security.

I*nstructions for encrypting data and files:*

Description of how to use encryption technology: All important and sensitive data will be encrypted with strong encryption algorithms such as AES (Advanced Encryption Standard) when stored and transmitted. Encryption will be performed on both data stored on the server and data in files when transmitted over the network.

Instructions for encrypting files and emails: Any important files containing sensitive information will be encrypted before being stored or shared. Emails containing sensitive information will also be sent through a secure channel, and if necessary, will be encrypted using methods such as S/MIME or PGP (Pretty Good Privacy).

**Cyber Attack**

*Common cyber attack prevention measures:*

Firewalls and Network Protection Measures: Poetry Publishing will deploy firewalls and network protection solutions such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to prevent cyber attacks from externally and detect abnormal behavior in the system.

Periodic System Updates: Company systems and software will be periodically updated with the latest security patches to protect against known security vulnerabilities.

Continuous System Monitoring: Poetry Publishing will deploy a continuous network monitoring system to detect unusual and potential hacker activities in the system.

Employee Training on Phishing and Intrusion Prevention: Employees will be trained on how to recognize and prevent common attack techniques such as phishing, spoofing, and social engineering.

*Cyber security incident handling process:*

Incident Detection and Reporting: All employees will be encouraged to report immediately if they detect any unusual activity in the system.

Incident Classification and Prioritization: Incidents will be classified and prioritized according to severity and potential to be handled as necessary.

Response and Recovery: A detailed incident response plan will be implemented to handle incidents effectively and quickly. After the problem is resolved, the system will be restored to its normal state.

Learning and Improvement: Each incident will be evaluated after resolution to learn and improve future incident prevention processes.

**Security Training and Awareness:**

Information security training program for new employees: Poetry Publishing will organize an information security training program for all new employees, helping them understand security risks and measures, as well as regulations. company policies and regulations related to information security.

Update information security knowledge and skills periodically for employees: The company will organize periodic training sessions and seminars to update information security knowledge and skills for employees. This includes learning from real-life incidents and new trends in the security field.

**Incident Management and Data Recovery:**

Security incident reporting and handling process: A detailed process will be established for reporting and handling security incidents. All employees will be instructed on how to report incidents and designated communication channels will be identified to ensure quick and effective incident handling.

Post-incident data recovery plan: Poetry Publishing will develop and maintain a detailed data recovery plan, including periodic backup measures and post-incident data recovery procedures to ensure that Any important information can be recovered safely and quickly.

**Continuous Evaluation and Improvement:**

Information security performance assessment methods: Poetry Publishing will perform periodic assessments of the system's information security performance, including security vulnerability testing, security policy compliance testing, and assess security risks.

Continuous improvement process for security systems: Based on the results of assessments, Poetry Publishing will develop and implement continuous improvement measures for security systems, to enhance the ability to deal with threats. new threats and improve overall security performance.

**References and Supporting Documents:**

List of information security references and resources: A list of information security references and resources will be provided to employees, including books, articles, and guidance documents. , and online documents.

Contact information for security support: A phone number and email address will be provided to employees so they can contact the company's security support if they need support or make a report about security issues.