

HUMAN RESOURCES DEPARTMENT

PRIVACY NOTICE SEC INTERNSHIP PROGRAM

The Securities and Exchange Commission is committed to protecting and respecting your personal data privacy. We are at the forefront of not only implementing but also complying with the Data Privacy Act of 2012 (RA No. 10173) and pertinent issuances of the National Privacy Commission (NPC).

This Privacy Notice outlines how the Human Resources Management Division (HRMD) of the Human Resources Department (HRD) collects, uses, and protects the personal information of internship applicants in connection with their applications.

1. What personal information do we collect from internship applicants?

The SEC collects from internship applicants personal and sensitive personal information necessary for their application and participation in the SEC Internship Program, such as but not limited to:

- **Personal identification:** Full name, birth date, birth place, sex, and signature;
- **Contact information:** Home address, mobile/telephone number, and email address;
- **Educational background:** Name of school/university, course or major, and year level; and
- **Emergency contact information:** Name and contact number of a person to notify in case of an emergency.

2. Why do we need to collect personal information?

As required by the Commission on Higher Education Memorandum Order No. 104, s. 2017, and the Implementation Guidelines of the SEC Internship Program, among others, the personal information collected from internship applicants shall be used for the following specific purposes:

- To evaluate qualifications and suitability:** To process an applicant's information to determine their fitness for the SEC Internship Program. The SEC evaluates applications based on eligibility requirements, relevance of academic study, and the level of interest and motivation to contribute to the work of the agency. The SEC also considers institutional representation and gender in the overall intern selection process.
- To facilitate communication:** To use the applicant's contact details to communicate regarding the status of their application, schedule interviews or orientation, and provide other updates related to the internship program.
- To draft the internship agreement:** For successful applicants, the collected information is used to prepare and draft the SEC Internship Program Agreement, which outlines the terms and conditions of the internship.
- For program administration and record-keeping:** To manage the intern's participation in the program, maintain official records, and coordinate with the intern's educational institution as may be required.

3. When do we collect personal information?

Personal information is primarily collected upon application by the internship applicants. The initial set of personal information is collected when an applicant submits their application and required documents through official channels and career fairs.

4. How do we collect personal information?

The SEC collects, uses, and/or processes personal information based on electronic and paper documents submitted by internship applicants. Specifically, the SEC collects personal information through the following methods:

- a. **Directly from applicants:** Personal information is collected when applicants directly provide it by:
 - Submitting an application and supporting documents via email to internship@sec.gov.ph or during career fairs; and/or
 - Uploading credentials and filling out application forms on the official SEC Internship Program Google Forms.
- b. **Through the applicant's educational institution:** In cases where an internship is facilitated through a formal school partnership or endorsement, the SEC may receive an applicant's personal information and credentials (such as endorsement letters, resumes, or transcripts of records) directly from an authorized representative of their college or university.

5. How do we store the data collected?

The SEC ensures the protection of personal data against accidental or unlawful destruction, alteration, disclosure, and other unlawful processing by implementing appropriate security measures.

The security and integrity of all data collected are ensured through the development and implementation of clear handling policies and procedures. These policies mandate specific physical security measures, including storing all physical applicant records in locked cabinets within the HRD-HRMD, restricting access to authorized HRD-HRMD personnel only, and enforcing a strict clean desk policy. Furthermore, electronic security protocols are in place for all electronic applicant records, such as resumes or scanned copies of transcript of records. These protocols require storage in a dedicated, access-controlled folder, prohibit storage on personal laptops, and enforce data protection through strong passwords and regular backups to prevent loss.

Personal information of SEC personnel is retained and disposed of in accordance with civil service laws and the National Archives of the Philippines Act of 2007 (RA No. 9470).

6. How do we dispose of the data collected?

Once a record has passed its retention period and is no longer needed, all hard and soft copies of personal information will be securely disposed of and destroyed in accordance with the SEC's Records and Disposition Schedule. Authorized disposal methods for physical documents (hard copies) include shredding or burial. Digital files (soft copies) must be permanently deleted using secure methods. The disposal will be carried out in the presence of a Records Management Analyst from the National Archives of the Philippines (NAP), an SEC Commission on Audit (COA) representative, and members of the SEC Records Management Improvement Committee (RMIC), such as the Chairperson, Vice-Chairperson, and relevant Departmental Directors/Records Focals (or their alternates).

7. What are the risks involved in processing your personal information?

Risk refers to the potential for incidents that may harm a data subject or organization, including unauthorized collection, use, disclosure, or access to personal data. It involves threats to the confidentiality, integrity, and availability of personal data or violations of data privacy principles and rights.

The SEC implements physical, technical, and organizational security measures to protect personal data but acknowledges that risks like cyberattacks, malware, and unauthorized access to manual records may still occur.

Adequate policies are in place to manage security incidents, in alignment with NPC policies, circulars, and other relevant issuances.

8. How do we keep your personal information secure?

Only authorized SEC personnel are granted access to the personal information collected by the HRD-HRMD. The collected personal information via the Internet or other electronic methods is stored in a secured database. We use reasonable security safeguards to protect the information gathered from any loss, unauthorized access, use, or disclosure. Specifically:

- a. We strictly adhere to clear policies on recruitment, selection, and placement, as well as the HRD's operational guidelines for handling personal information and the SEC's Data Privacy Manual.
- a. Physical application documents are stored in secure, locked cabinets within the HRD-HRMD. Access to the 201 file room is restricted to authorized personnel only, i.e., personnel of the Human Resource Information and Services Unit of the HRD-HRMD.
- b. We enforce a clean desk policy to ensure that documents containing your personal information are never left unattended or unsecured. Furthermore, we maintain a clean, organized, and efficient workplace by implementing and adhering to the 5S methodology (sort, set in order, shine, standardize, sustain). This practice helps minimize the risk of data breaches and enhances overall security.
- b. Electronic records are held in a secured database and dedicated digital folders with robust access controls. To prevent unauthorized copies and disclosure, storing application files on personal laptops or devices is strictly prohibited. We utilize strong password policies for all systems, and regular data backups are performed to prevent accidental loss. These comprehensive safeguards are designed to protect your personal information from any loss, unauthorized access, use, or disclosure.

9. What are the rights of the data subjects?

Under the Data Privacy Act of 2012, a data subject refers to an individual whose personal information is collected and processed. We are duly bound to observe and respect your privacy rights, including your right to information, right to access, right to object, right to correct, right to remove, right to damages, right to file a complaint, and right to data portability.

10. How can data subjects exercise these rights?

Data subjects are informed of their rights through this Privacy Notice, which also cites the legal basis for processing their personal information. Should they wish to exercise other rights, such as the right to access, right to object, right to correct, right to remove, right to damages, right to file a complaint, and right to data portability, they may file a request with the SEC Data Protection Officer (DPO). They may contact the DPO at 8818-7204 or send an email or to dpo@sec.gov.ph.

FEEDBACK ON THE PRIVACY NOTICE

If you have any questions, concerns, or requests related to this Privacy Notice, or if you would like to exercise your rights under applicable data protection laws, please contact our Data Protection Officer, Director Oliver V. Chato:

- **Email:** dpo@sec.gov.ph
- **Phone:** 8818-7204

CONSENT FORM

I hereby acknowledge that I have read and understood the SEC Privacy Notice for the SEC Internship Program.

I freely and voluntarily consent to the processing of my personal information by the SEC for purposes related to my internship application and the administration of the SEC Internship Program, including but not limited to:

1. Assessing my qualifications and suitability as a student-intern for the program;
2. Preparing and drafting the SEC Internship Program Agreement, which is required for entering into the internship, should my application be successful; and
3. Contacting me regarding my application status, interview schedules, and other related activities.

Furthermore, I expressly authorize my educational institution to release and disclose any and all information concerning me that may be relevant to my application as a student-intern with the SEC.

I understand that I have the right to withdraw my application and my consent to the processing of my personal information at any time.