	Document Name:	Date:
	DATA HANDLING POLICY	1 October 2021
		Page: 1 of 5
		IT Department

1. OBJECTIVE

This policy ensures that controls are in place to manage the risks to confidentiality, integrity, and availability of company confidential data of any form and represent a minimum standard for protection of these data.


2. COVERAGE

This policy covers all employees of the companies in the PHINMA Group.

3. CATEGORIES OF COMPANY INFORMATION

The following are categories of company information based upon the intended use and expected impact if disclosed:

- **Public:** Information intended for public use that, when used inappropriately, would have little to no effect on the operations, assets, or reputation of the company, or its obligations concerning data privacy. Examples of public information are brochures, website contents, social media contents, and newsletters.
- **Internal:** Information not intended for parties outside the company that, if disclosed, could result in moderate level of risk on the operations, assets, or reputation of the company, or its obligations concerning data privacy. Examples of internal information are company policies, internal memorandums, and sales information.
- **Confidential:** Information intended for limited use within the company that, if disclosed, could result in adverse effects on the operations, assets, or reputation of the company, or its obligations concerning data privacy. Examples of confidential information are employee information, information covered by confidentiality agreements, unreleased company information, undisclosed financial statements, proprietary data, trade secrets, pricing information, customer information, and other information that can be used to the disadvantage of the company.

	Document Name:	Date:
	DATA HANDLING POLICY	1 October 2021
		Page: 2 of 5
		IT Department

4. POLICY STATEMENT

4.1. Creation and Identification of Data


- 4.1.1. Employees shall create data as part of the normal course of conducting the business of the company. Employees shall maintain these data appropriately throughout their entire lifecycle.
- 4.1.2. Department heads shall identify and label appropriately all company data in their possession, whether Confidential, Internal, or Public.

4.2. Access to Confidential Information

- 4.2.1. Only employees who have authorization from the department head shall have access to confidential information. When working with confidential data, the following rules shall apply:
- Reproduction of unofficial copies is not allowed.
 - Where access to confidential data is authorized, use of such data shall be limited to the purpose required to perform the job functions.
 - Employees shall abide by the applicable laws and company policies. Ethical restrictions shall be applied at all times.
 - Any other form of access or disclosure of confidential information requires the written approval of the department head.
- 4.2.2. Department heads shall monitor the access to confidential data.
- 4.2.3. Department heads shall notify the IT Department on termination of authorized access to confidential information by an employee.

4.3. Use

- 4.3.1. Employees shall observe confidentiality when discussing or displaying confidential company information.
- 4.3.2. When printing or photocopying a document, employees shall ensure that only authorized personnel will be able to see the output.

	Document Name:	Date:
	DATA HANDLING POLICY	1 October 2021
		Page: 3 of 5
		IT Department

4.3.3. The IT Department shall follow an established and documented software development lifecycle when building software applications that process confidential information.

4.4. Storage

4.4.1. Employees shall ensure that keys and access cards for rooms or file cabinets are not accessible from unauthorized personnel.

4.4.2. Employees shall not remove digital or physical confidential documents from its approved secure location without written approval from the department head. In the event that a confidential information is required to be removed from its location, the information (whether electronic or paper) must be protected at all times from accidental or malicious disclosure.

4.4.3. Employees shall password-protect files containing confidential information when stored at cloud-based, company network, or assigned computer file storage.

4.4.4. Employees shall avoid storing confidential data on mobile devices (i.e. external hard drives, mobile phones, tablets, thumb drives, memory cards, and the like). Seek an approval from the department head and the IT Department when storing of company data to the mobile devices is required.


4.5. Digital Transmission

4.5.1. Employees shall only send confidential information via encrypted channel. When attaching a confidential document to an email, ensure that it is password-protected. Sending of confidential information via instant message or unsecured file transfer is not allowed.

4.5.2. Employees shall properly label internal and confidential information to be sent to all recipients.

4.6. Physical Transport

4.6.1. When sending physical confidential documents, the employees shall avail from a reputable courier service providers. Ensure that the package can be tracked, duly signed by the receiving party, and tamper-evident seal is used. Obfuscation of the confidential documents must be done.


	Document Name:	Date:
	DATA HANDLING POLICY	1 October 2021
		Page: 4 of 5
		IT Department

4.7. Retention of Confidential and Personal Information

- 4.7.1. Permanent records shall be kept by the data owners or department heads.
- 4.7.2. Inactive non-permanent records shall be archived by the employees and kept only within retention period.
- 4.7.3. The department head is responsible for tracking the company information to ensure that confidential and personal data shall not be retained longer than necessary.
- 4.7.4. For the standard retention schedule, please refer to **Annex A** of this document.

4.8. Disposal of Records, Media, and Equipment

- 4.8.1. Employees shall shred (cross-cut shredding is recommended) all confidential hardcopy documents and transitory work products (e.g., unused copies, drafts, and notes).
- 4.8.2. Employees shall physically destroy removable storage media, such as CDs, DVDs, external hard drives, mobile phones, tablets, thumb drives, memory cards, and the like, to ensure that no data is accessible by other parties.
- 4.8.3. For computer equipment disposal, employees shall seek assistance from the IT Department which shall apply physical destruction techniques or DOD-approved data wiping method.

	Document Name: DATA HANDLING POLICY	Date: 1 October 2021
		Page: 5 of 5
		IT Department

5. EFFECTIVITY

This policy is effective immediately and in force until such time that it is amended by PHINMA, taking into account its applicability to the current business situation and to the needs of the PHINMA Group.