PILAPIL, MIGUEL V. **INFORMATION ASSURANCE & SECURITY 1**
3-BSIT-2 **LABORATORY EXP: DATA PRIVACY ACT #6**

1. What is the importance and purpose of the Republic Act 10173 known as Data Privacy Act of 2012 in the field of IT?

- The importance and the purpose of R.A 10173 known as data privacy is to protect personal data in information and communications systems both in the government and the private, personal, sensitive information.

2. What are the scopes of the Data Privacy Act?

- The scopes of the data privacy act applies to any natural or juridical persons involved in the processing of the personal information.

3. Explain the Security of Personal Information.

- The security of personal information, known as data security or information security, is protecting sensitive and confidential data from unauthorized access, disclosure, alteration, and destruction, by ensuring the security of personal information is crucial to safeguarding individuals and privacy, preventing identity theft and maintain trust in digital systems and services, additionally there are consider measure for securing the personal information:

  1. Data Encryption: use encryption protocols like TLS/SSL to secure data while transmitted over networks.
  2. Access Control: implement the strong access controls by assigning unique, username and password or other authentication methods to individuals.
  3. Physical Security: securing physical access to servers, data centers, and storage facilities to prevent unauthorized tampering or theft.
  4. Network Security: use firewalls, intrusion detection system, and intrusion prevention system to protect networks from unauthorized.
  5. Regular Updates or Patch: keeping operating systems, software, and applications up to date with security patches and updates to mitigate known vulnerabilities.

  And there are many consider for securing the personal information, security audits and monitoring, employee training and awareness, and data backup & recovery, legal and regulatory compliance, data disposal, vendor and third party security, data minimization and retention all of the is security measures should be tailored to specific needs and risks of your organization, and should be reviewed and updated annually or regularly to adapt to evolving security threats and technologies.

4. Discuss the SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT.

- The Security of sensitive personal information in government is a critical aspect of maintaining trust, safeguarding citizens privacy, and ensuring the protection of functioning government agencies, and governments collect and handle a vast amount of personal information or data, including social security numbers, healthcare records, tax information, and more are security of this data is paramount, and here are also overview what governments secure the sensitive personal information:

  1. Legal and regulatory framework, governments often have stringent laws and regulations in place to govern the collection, storage, processing, and sharing of personal information, these laws may impose specific requirements for data protection and security.
  2. Data classification and handling, governments classify data based on sensitivity, personal information is treated with the highest level of security, and with access restricted to authorized personnel only.
  3. Access control, access to government systems and databases containing sensitive personal information is controlled through strict access controls, and includes user authentication, or role based access control, by principle of least privilege.
  4.Encryption, data encryption is employed to protect data both in transit and the rest, ensures that even if data is intercepted or compromised, it remains unreadable without the proper decryption keys.
  5. Security policies and procedures, government agencies establish comprehensive security policies and procedures that outline security best practices, incident to response plans and guidelines for employees and contractors handling sensitive data.
  6. Network security, government networks are protected by firewalls, IDS & IPS safeguard against unauthorized access and cyber threats.
  7. Regular audits and assessments, government agencies conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in their systems and networks.
  8. Secure data disposal, secure procedures are in place to dispose of sensitive information when it is no longer needed.
  9. Data sharing agreements, sharing personal information with other government agencies or external partners, strict data sharing agreements are established to ensure the data is handled securely and in compliance with applicable laws and regulations.
  10. Secure procurement, procuring IT systems or services, government agencies prriotize security in the selection and vetting of vendors.

5. What are the Penalties in this Republic Act?

- The penalties in this republic act 10173 are known data privacy act of 2021 in philippines, are many various penalties for violations of its provisions, these are penalties intended to ensure compliance with the law and to protect the privacy and security of individuals personal information.

  1. Fines for unauthorized processing or disclosure, including obtaining, accessing, without consent of the data subject is subject to fine range from PHP 500,000 to 2,000,000 for each violation.
  2. Criminal penalties for unauthorized processing or disclosure, can lead to criminal penalties, including imprisonment, individuals found guilty of violating the law may face imprisonment of up to six years.
  3. Penalties for unauthorized access or intentional breach, such as hacking into systems or databases, can result in fines and imprisonment, the penalties can range from PHP 500,000 to 4,000,000 and imprisonment up to six years.
  4. Penalties for negligent or inadequate data protection, organizations that are negligent in protecting personal data or fail to implement reasonable security measures can be fined up to PHP 1,000,000, this penalty is meant to encourage organizations to take data security seriously.
  5. Non-monetary penalties, the NPC or national privacy commission has the authority to impose non-monetary penalties, such as suspension of personal data processing, on organizations found in violation of Data privacy act.
  6. Liability of directors and officers, and other responsible parties of an organization can also be held criminally liable for violations of the law, this emphasizes the accountability of individuals in positions of authority.