

# INFORMATION SECURITY POLICY

## INFORMATION SECURITY POLICY

Perbadanan Bekalan Air Pulau Pinang Sdn. Bhd. (PBAPP) recognises the value and importance of information and Information Assets for the organisation in providing adequate clean and safe water to the state of Penang. This Policy is aimed at protection of Information Assets of Sungai Dua Water Treatment Plant (WTP) and all its supporting services which shall serve as point of reference for all other subsequent policies pertaining to Information Security and shall also act as a guide towards planning for emergency and crisis situations.

### The Management of PBAPP is committed to ensuring that:

1. All Information Assets are adequately protected against unauthorised access.
2. The confidentiality, integrity, and availability of information and Information Assets are consistently maintained and safeguarded.
3. All Information Assets shall be classified appropriately, and Risk Management processes shall be conducted to identify, assess, and evaluate security risks to ensure that suitable control measures are implemented.
4. Appropriate standards, procedures, and guidelines on information security are established and maintained to support effective implementation and to define the minimum compliance requirements for all employees and third parties conducting business with Sungai Dua WTP.
5. All applicable regulatory and legislative requirements shall be complied with at all times.
6. Information security training and awareness programmes shall be made available to all staff of the Sungai Dua WTP.
7. Continual improvement of the Information Security Management System (ISMS) shall be pursued through ongoing enhancement of security initiatives and the provision of adequate resources.

### Application of this Policy

1. This Policy applies to all staff of the Sungai Dua WTP and its supporting services, as well as to all information contained therein—whether owned by Sungai Dua WTP, held in custody on behalf of customers, or used by Sungai Dua WTP and its supporting services.
2. The ISMS Management Representative (ISMS MR) is responsible for establishing and overseeing information security within the Sungai Dua WTP and its supporting services. The ISMS MR shall also maintain the policy and advise on its implementation.
3. All Department Heads are directly responsible for implementing this Policy within their respective departments and ensuring their staff's compliance.
4. All employees of Sungai Dua WTP are required to comply with the Policy, as well as with all related standards, procedures, and guidelines. Any breach may result in disciplinary action.
5. All staff shall promptly report any actual or suspected information security breaches to their respective Managers for appropriate action.