IT GOVERNANCE NETWORK

# Protection of Personal Information Act
# Information Security

## COMPLYING WITH THE PROTECTION OF PERSONAL INFORMATION ACT

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable **technical and organisational measures** to prevent loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

### Generally accepted Information Security practices and procedures

A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures against the identified risks.

ISO/IEC 27001 is an international standard for information security management. It is widely recognised as the generally accepted framework to plan, implement and manage the technical and organisational measures that responsible parties are required to take to protect personal information.

The Information Regulator is more likely to consider that the responsible party has taken reasonable steps to prevent a contravention if the responsible party can demonstrate compliance with the ISO/IEC 27001 standard on information security management in the areas relevant to the contravention.

### Information Security Risk Assessment

A responsible party is required to take reasonable measures to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.

If a contravention should occur, the Information Regulator is more likely to consider that the responsible party has taken reasonable steps if the responsible party can provide evidence that a risk assessment had been carried out, the responsible party had recognised the risks of handling personal data, had taken steps to address these risks and had given advice and guidance to the responsible staff.

ISO/IEC 27001 requires a risk based approach to managing information security. First an inventory of information assets within scope must be prepared. Thereafter, the threats vulnerabilities and impact on privacy are established, options to treat the risks are identified and a risk treatment plan developed.

Responsible parties should have good governance and audit arrangements in place to minimise the impact of a breach.

### Technical Safeguards against identified security risks

Technical measures that a responsible party can take against identified threats include:

- Physical protection
- Secure hardware
- Resource protection
- Secure data in distributed environments
- Access control
- Application controls
- Cryptographic services
- Malicious code detection tools
- Secure data exchange
- Effective data destruction measures
- System design and development controls.

### Organisational Safeguards against identified risks

Organisational measures that a responsible party can take against identified threats include:

- Comprehensive information security policy and plan
- Internal security organisation and architecture
- Information security management system
- Responsibilities assigned for protecting information assets
- Information security risk assessment
- Information classification scheme
- Security operating procedures
- Staff education
- Security incident response procedures
- Business continuity management arrangements
- Security compliance reviews
- Information system audits
- Management reviews of counter-measure effectiveness.

### Security measures regarding information processed by an Operator (i.e. service provider)

A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator (service provider) which processes personal information for the responsible party establishes and maintains the necessary technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. Thereafter the responsible party must notify the Regulator and the data subject as soon as reasonably possible after the discovery of the compromise.

The notification to a data subject must be in writing.

### Managing an information security breach

Almost daily there are new reports about hundreds or thousands of records of personal information being accessed by unauthorised personnel and improperly disclosed, used or manipulated.

Correctly responding to an information security breach is a cornerstone of protecting a data subjects rights. Failure to do so correctly may have severe consequences for the responsible party. These may include financial settlements, administrative fines, criminal charges, penalties and civil action for damages, regardless of whether or not there is intent or negligence on the part of the responsible party.

More significant to a responsible party could be the loss of trustworthiness and respect, reputational damage and loss of business.

 