## SECURITY REQUIREMENTS

**What security obligations are imposed on data controllers and data processors?**

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties. Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.

Employers in the Philippines should implement organizational, physical and technical measures to protect personal data. Per the Data Privacy Act of 2012 (Ch. 5, Sec. 20), security measures should be determined based on factors including the nature of the data, risks associated with processing, the cost of implementation, current best practices and the organization's size.

Organizational measures should include (Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule VI, Sec. 26):

- designating a Compliance Officer or Data Protection Officer;
- data protection policies;
- documenting and recording the data processing system and activities;
- managing, supervising and training employees on how to process, handle, store and access personal data.

Examples of physical measures should include (Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule VI, Sec. 27):

- implementing policies and procedures to monitor and limit physical access as well as limiting activities in the room/workstation/facility. This includes guidelines relating to the proper use of and access to electronic media;
- designing workspaces to provide privacy to anyone processing personal data; and,
- securing data against natural disasters, power disturbances, external access, mechanical destruction of files and equipment, etc.

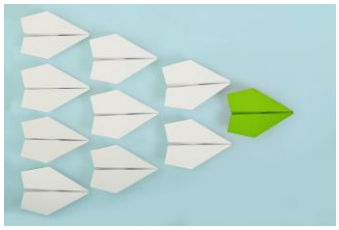
Technical security measures are policies designed to protect computer systems and should include the maintenance of confidentiality, integrity, availability, and resilience of the processing systems and services (Implementing Rules and Regulations of the Data Privacy Act of 2012, Rule VI, Sec. 28).

In addition to the above, certain measures are recommended by the National Privacy Commission,

such as (Circular 16-03 Personal Data Breach Management):

- creating a data breach response team;
- implementing back-up solutions;
- controlling access and securing log files;
- encryption; and,
- a record return/disposal policy (i.e. record retention policy).

Employers must ensure that third-parties and employees who process personal data follow the same security measures and confidentiality protocols.



**HR Best Practices**:

Employee data protection should be built into the organizational framework. As part of these efforts, regularly train employees who may have access to personal information to ensure that they are following all technical, physical and organizational security measures.

When working with sub-contractors and other third-party processors, ensure contracts with service providers detail the security and confidentiality measures that will be implemented.

Last updated December 2020.