

Pillar 4: Be Accountable:

Implement your Privacy & Data Protection (PDP) Measures

Legal Basis: Sec. 20.a-e, 22 and 24 of the DPA, Sections 25-29 of the IRR,
Circular 16-01

Maintaining confidentiality, integrity, and availability	Insufficient controls to maintain confidentiality, integrity, and availability
<ul style="list-style-type: none"><input type="checkbox"/> Data protection risks have been identified and documented<input type="checkbox"/> Appropriate and up-to-date organizational, physical, and technical controls are in place to manage these risks (e.g ISO:IEC 27002)<input type="checkbox"/> Data protection policies are cascaded throughout the organization and updated as needed<input type="checkbox"/> Vulnerability scanning is conducted at least once a year<input type="checkbox"/> Business continuity drills are conducted at least once a year<input type="checkbox"/> For data stored outside the Philippines, location of foreign country is defined<input type="checkbox"/> For personal data stored in the cloud, NPC recommends that provider is ISO:IEC 27018 compliant (from Circular 16-01)<input type="checkbox"/> For digitized personal data, NPC recommends 256-bit AES for data at rest and in transit (from Circular 16-01)	<ul style="list-style-type: none"><input type="checkbox"/> Controls for data protection are not appropriate for the risks identified<input type="checkbox"/> Controls for data protection are not updated for new risks/threats<input type="checkbox"/> Controls for data protection are not complied with<input type="checkbox"/> Cyber-hygiene practices are lax<input type="checkbox"/> Business continuity drill has not been conducted in the last 12 months<input type="checkbox"/> Security vulnerability scanning has not been conducted in the last 12 months

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

SECTION 5. CLOUD FIRST POLICY

- 5.1 Cloud computing has brought a new and more efficient means of managing government information technology resources. It is hereby declared the policy of the government to adopt a “cloud first” approach and for government departments and agencies to consider cloud computing solutions as a primary part of their infostructure planning and procurement.
- 5.2 All government agencies shall adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government online services, except:
- 5.2.1 When it can be shown that an alternative ICT deployment strategy meets special requirements of a government agency; and
 - 5.2.2 When it can be shown that an alternative ICT deployment strategy is more cost effective from a Total Cost of Ownership (TCO) perspective and demonstrates at least the same level of security assurance that a cloud computing deployment offers.

DICT Circular
2017-002

18 January 2017

DEPARTMENT CIRCULAR
NO. 2017 - 002

SECTION 12. DATA SOVEREIGNTY

The benefits of cloud are best realized when there is no data residency restrictions placed on data. Data residency restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure. Nevertheless, where agencies have concerns with extraterritorial access to data or where Tier 3 Confidential and above-Sensitive Data are involved, then the appropriate security standards and controls should be employed or the agency should work with DICT to consider deploying a private, on-premise cloud solution.

SECURITY CONTROLS	BASELINE CERTIFICATION AND/OR PROTOCOL REQUIRED	DESCRIPTION
Security Assurance Requirements	<ul style="list-style-type: none"> • ISO/IEC 27001 - Information Security Management • Payment Card Industry (PCI) Data Security Standard (DSS) • <i>Optional: Service Organization Control (SOC) 1 and 2</i> • <i>Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i> 	<p>These are the baseline and <i>optional</i> Security Assurance Requirements for Cloud Service Providers to be accredited on GovCloud.</p> <p>These Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.</p>
Encryption Requirements	<ul style="list-style-type: none"> • AES (128 bits and higher) • TDES (minimum double-length keys) • RSA (1024 bits or higher) • ECC (160 bits or higher) • ElGamal (1024 bits or higher). 	<p>These are the baseline Encryption Requirements for Government Workloads before being deployed on an accredited GovCloud Cloud Service Provider. Note that while Cloud Service Providers can provide services with such Encryption technologies built in, these technologies can also be deployed by Government Agencies on such Workloads.</p>

RA 10173, Sec. 23 (b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive

Circular 16-01.

SECTION 10. When a government agency engages a service provider for the purpose of storing personal data under the agency's control or custody, the service provider shall function as a personal information processor and comply with all the requirements of the Act, its IRR and all applicable issuances by the Commission.

SECTION 12. The Commission recommends ISO/IEC 27018 as the most appropriate certification for the service or function provided by a service provider under this Rule.

The National Privacy Commission of the Philippines recommends the following standards:

ISO:IEC 27002

- As the standard to assess control gaps in data protection framework
- Ref: Section 6, NPC Circular 16-01

ISO:IEC 27018

- as the most appropriate certification for a service provider
- Ref: Section 12, NPC Circular 16-01

AES 256

- As the standard for encrypting personal data, at rest and in transit
- Ref: Section 8, NPC Circular 16-01

Multi-factor authentication

- As the standard for allowing online access to personal data
- Ref: Section 18, NPC Circular 16-01

ISO 27001 vs 27018 Benefits

27001 – your data is stored in your own data center

- You have a clear picture of what your information security risks are
- You can identify a set of controls to manage your risks
- You can monitor the ongoing implementation and deployment of the selected controls

27018 – your data is stored in someone else's data center

- You have control over which country your data will be stored in
- Your data won't be used for marketing or advertising without your consent
- You will be notified of legal requests for data disclosure

Circular 16-01, Sections 7 to 13

Processing of Personal Data

“Owned” Data Center

- Covered as PIC
- Subject to NPC Audit (Sec. 11)
- AES-256 Encrypted (Sec. 8)
- Access control system (Sec. 9)
- Archives are also covered (Sec. 13)
- ISO 27001/27002

“Non-owned” Data Center

- Covered as PIP (sec. 10)
- Subject to NPC Audit (Sec. 11)
- ISO 27018 (Sec. 12)
- AES-256 Encrypted (Sec. 8)
- Archives are also covered (Sec. 13)
- Contract subject to review (Sec. 7)
- If data is stored outside the country, geographic location must be specified in contract (IRR, Sec. 44.a)

Other recommendations

- A. Limit access to data to authorized users, devices, and programs (*Circular 16-01, Sections 14 to 21*)
- B. Apply similar security and access controls to non-digitized files/media (*Circular 16-01, Section 22*)
- C. Use secure channels when transferring personal data (*Circular 16-01, Sections 24 to 29*)
- D. Observe proper procedures for disposal/archiving of personal data (*Circular 16-01, Sections 30 to 32*)

The era of cyber-disaster may finally be here

By [Adam Taylor](#) May 15 at 1:00 AM [✉](#)



On Friday, the world was hit by one of the biggest cyberattacks in recent history.

Ransomware

- What is ransomware?
 - Your data is forcibly encrypted
 - If you want your data back, you have to pay
- How avoid this threat?
 - Use licensed software and have auto-update on
 - Don't click on links, type in the URL
 - Check with senders before opening attachments
 - Backup, backup, backup!

Summary

- Integrate data privacy risk into:
 - security risk assessments
 - Information systems security policy
 - corporate security policy (protection of physical premises and hard assets)
 - business continuity plans
- Maintain security measures
 - Technical (e.g. intrusion detection, firewalls, monitoring, encryption)
 - Physical (sight lines, facilities control, CCTVs, etc.)
 - Organizational (“acceptable use” policy, role-based access to personal information, segregation of duties, issuance and renewal of security clearances)
- Be proactive:
 - Data-loss prevention strategy
 - Regular testing of data security posture
 - Security certification (ISO/IEC)
 - Hire/train “ahead of the curve”



End of Module 5.
Any questions?