Republic of the Philippines
NATIONAL PRIVACY COMMISSION

DATA SECURITY AND COMPLIANCE OFFICE

Data Security and Technology Standards Division

ADVISORY ON THE ADOPTION OF INTERNATIONAL DATA PROTECTION STANDARD

NO. 2021-002

ISO/IEC 29151 – Information technology – Security techniques – Code of practice for personally identifiable information protection

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012, provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, pursuant to Section 7 of the Data Privacy Act of 2012, the National Privacy Commission is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers with the provisions of the Act and with international standards for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides that, among the Commission's functions, is to issue guidelines for organizational, physical and technical security measures for personal data protection, taking into account the nature of the personal data to be protected, the risks presented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, cost of security implementation, and the most appropriate standard recognized by the information and communications technology industry, as may be necessary;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this advisory on the adoption of ISO/IEC 29151 as guide in implementing controls for data protection.

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Scope of the International Standard (IS) [1]

This document establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of Personally Identifiable Information (PII).

In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII which may be applicable within the context of an organization's information security risk environment(s).

This document is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities, and not-for-profit organizations, which process PII.

Requirements

This IS provides additional implementation guidance for personal data protection that are in the Information Security Management System (ISMS) guidance in ISO/IEC 27002.

The same requirements found in the annex of ISO/IEC 27001 and ISO/IEC 27002 applies to this standard.

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Additional guidance of implementation for personal data protection can be seen in Annex B of this Advisory.

[1] https://www.iso.org/standard/62726.html
The scope is directly lifted from the International Standard (IS) document, terms may be different from the DPA, but it has a similar meaning to the DPA terms. Refer to Annex A for the comparison of terms.

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

The annex contains implementation guidance for the privacy principles stated in ISO/IEC 29100 – Privacy framework.

- Consent and choice
- Purpose legitimacy and specification
- Collection limitation
- Data minimization
- Use, retention and disclosure limitation
- Accuracy and quality
- Openness and transparency
- PII principal participation and access
- Accountability
- Information security
- Privacy compliance

Benefits

The number of organizations, whether in public or private sectors, managing personal data is increasing. The societal expectation for the protection of the individual's privacy and the security of data relating to the individual is increasing. The National Privacy Commission (NPC) released its first circular (NPC Memorandum Circular 16-01) about the security of personal data in government agencies last 2016. The NPC Circular 16-01 is issued to assist government agencies engaged in the processing of personal data and help implement more detailed policies and procedures, which reflect its specific operating requirements. Section 6 of this circular recommends the control set stated in ISO/IEC 27002 as the minimum standard to assess any gaps in the agency's control framework. This also provides guidelines for organizations that were able to conduct privacy impact assessments and implement the identified controls to mitigate the determined risks.

Annex C illustrates the relative subclauses of ISO/IEC 29151 to the NPC Circular 16-01 requirements.

For organizations that are already implementing or will be implementing the requirement and guidance on ISO/IEC 27001 and ISO/IEC 27002 respectively, this IS will help further enhance their control set as it gives a broad range of additional guidance in personal data protection.

Guide for Adoption

The IS provides guidelines in identifying and establishing controls specifically for data protection in addition to the guidelines stated in ISO/IEC 27002 and NPC Memorandum Circular 16-01 and it could be a suitable direction concerning the identified risks after conducting privacy impact assessments in implementing controls.

PICs and PIPs who will use this IS within their organizations shall still follow the DPA's terminologies, its IRR, and other relevant issuance. The guidance for comparing the terms is in Annex A. The IS does not amend the DPA, its IRR, and other relevant issuances of the NPC. In the event of a conflict between the provisions of the IS and the compliance requirements stated in the DPA, its IRR, and other relevant issuances of the NPC, the latter shall prevail.

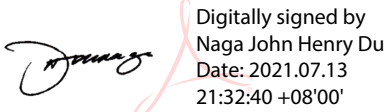
The IS were adopted as Philippine National Standards (PNS) by the Bureau of Philippine Standards (BPS) upon the recommendation of the Subcommittee on Information security, cybersecurity and privacy protection (SC 1) and the Technical Committee on Information Technology (BPS/TC 60). BPS/TC 60 is in charge of the review and adoption of relevant International Standards that will be distributed here in the Philippines.

The copy of the standards is available for a minimal fee at the Standards Data Center of the BPS – 3F DTI Bldg., 361 Sen. Gil Puyat Ave., Makati City. For quotation, please email BPS at bps@dti.gov.ph.

Recommended by:

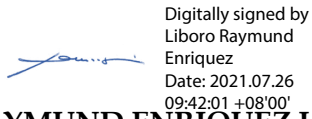
KELVIN S. MAGTALAS
OIC-Chief, DSTSD

Recommending Approval:



JOHN HENRY D. NAGA
OIC-Director, DASCO

Approved by:



RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Annex A – DPA and ISO/IEC 29100 Terms and definitions

	DPA of 2012	ISO/IEC 29100
Term	**Personal information**	**Personally Identifiable Information (PII)**
Definition	Refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.	any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal
Term	**Personal Information Controller (PIC)**	**PII Controller**
Definition	refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: 1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or 2. A natural person who processes personal data in connection with his or her personal, family, or household affairs; There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing; privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes	privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
Term	**Personal Information Processor (PIP)**	**PII processor**
Definition	refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Term	Data Subject	PII Principal
Definition	refers to an individual whose personal, sensitive personal, or privileged information is processed	natural person to whom the personally identifiable information (PII) relates. *Note: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal"*
Term	**Personal Data Breach**	**Privacy breach**
Definition	refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach maybe in the nature of: 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data; 2. Integrity breach resulting from alteration of personal data; and/or 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.	situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements
Term	**Sensitive Personal Information (SPI)**	**Sensitive PII**
Definition	refers to personal information: 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; 2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; 3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and 4. Specifically established by an executive order or an act of Congress to be kept classified.	category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal *Note: In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.*
Term	**processing**	**processing of PII**

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Definition	refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;	operation or set of operations performed upon personally identifiable information (PII) *Note: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.*
Term	**third party**	**third party**
Definition	*Mentioned but nit defined*	privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor
Term	**consent**	**consent**
Definition	refers to any freely given, specific, informed indication of will, hereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.	PII principal's freely given, specific and informed agreement to the processing of their PII

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Annex B –ISO/IEC 27002 and ISO/IEC 29151 Matrix

This table illustrates the clauses in 27002 and if it contains additional guidance for data protection in ISO/IEC 29151.

ISO/IEC 27002		ISO/IEC 29151		
Clause	**Title**	**Clause**	**Title**	**Additional guidance**
5	**Information security policies**	**5**	**Information security policies**	No
5.1	**Management direction for information security**	**5.1**	**Management directions for information security**	No
5.1.1	Policies for information security	5.1.2	Policies for information security	Yes
5.1.2	Review of the policies for information security	5.1.3	Review of the policies for information security	No
6	**Organization of information security**	**6**	**Organization of information security**	No
6.1	**Internal organization**	**6.1**	**Internal organization**	No
6.1.1	Information security roles and responsibilities	6.1.2	Information security roles and responsibilities	Yes
6.1.2	Segregation of duties	6.1.3	Segregation of duties	Yes
6.1.3	Contact with authorities	6.1.4	Contact with authorities	Yes
6.1.4	Contact with special interest groups	6.1.5	Contact with special interest groups	No
6.1.5	Information security in project management	6.1.6	Information security in project management	Yes
6.2	**Mobile devices and teleworking**	**6.2**	**Mobile devices and teleworking**	No
6.2.1	Mobile device policy	6.2.2	Mobile device policy	Yes
6.2.2	Teleworking	6.2.3	Teleworking	No
7	**Human resource security**	**7**	**Human resource security**	No
7.1	**Prior to employment**	**7.1**	**Prior to employment**	No
7.1.1	Screening	7.1.2	Screening	No
7.1.2	Terms and conditions of employment	7.1.3	Terms and conditions of employment	No
7.2	**During employment**	**7.2**	**During employment**	No
7.2.1	Management responsibilities	7.2.2	Management responsibilities	Yes
7.2.2	Information security awareness, education and training	7.2.3	Information security awareness, education and training	Yes
7.2.3	Disciplinary process	7.2.4	Disciplinary process	Yes

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

7.3	**Termination or change of employment**	**7.3**	**Termination or change of employment**	No
7.3.1	Termination or change of employment responsibilities	7.3.2	Termination or change of employment responsibilities	No
8	**Asset management**	**8**	**Asset management**	No
8.1	**Responsibility for assets**	**8.1**	**Responsibility for assets**	No
8.1.1	Inventory of assets	8.1.2	Inventory of assets	Yes
8.1.2	Ownership of assets	8.1.3	Ownership of assets	No
8.1.3	Acceptable use of assets	8.1.4	Acceptable use of assets	Yes
8.1.4	Return of assets	8.1.5	Return of assets	No
8.2	**Information classification**	**8.2**	**Information classification**	No
8.2.1	Classification of information	8.2.2	Classification of information	Yes
8.2.2	Labeling of information	8.2.3	Labeling of information	Yes
8.2.3	Handling of assets	8.2.4	Handling of assets	Yes
8.3	**Media handling**	**8.3**	**Media handling**	No
8.3.1	Management of removable media	8.3.2	Management of removable media	Yes
8.3.2	Disposal of media	8.3.3	Disposal of media	Yes
8.3.3	Physical media transfer	8.3.4	Physical media transfer	Yes
9	**Access control**	**9**	**Access control**	No
9.1	**Business requirements for access control**	**9.1**	**Business requirements for access control**	No
9.1.1	Access control policy	9.1.2	Access control policy	No
9.1.2	Access to networks and network services	9.1.3	Access to networks and network services	No
9.2	**User access management**	**9.2**	**User access management**	No
9.2.1	User registration and de-registration	9.2.2	User registration and de-registration	Yes
9.2.2	User access provisioning	9.2.3	User registration and de-registration	Yes
9.2.3	Management of privileged access rights	9.2.4	Management of privileged access rights	Yes
9.2.4	Management of secret authentication information of users	9.2.5	Management of secret authentication information of users	No
9.2.5	Review of user access rights	9.2.6	Review of user access rights	No
9.2.6	Removal or adjustment of access rights	9.2.7	Removal or adjustment of access rights	No
9.3	**User responsibilities**	**9.3**	**User responsibilities**	No
9.3.1	Use of secret authentication information	9.3.2	Use of secret authentication information	No
9.4	**System and application access control**	**9.4**	**System and application access control**	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

9.4.1	Information access restriction	9.4.2	Information access restriction	Yes
9.4.2	Secure log-on procedures	9.4.3	Secure log-on procedures	Yes
9.4.3	Password management	9.4.4	Password management	No
9.4.4	Use of privileged utility programs	9.4.5	Use of privileged utility programs	No
9.4.5	Access control to program source code		Access control to program source code	No
10	**Cryptography**	**10**	**Cryptography**	No
10.1	**Cryptographic controls**	**10.1**	**Cryptographic controls**	No
10.1.1	Policy on the use of cryptographic controls	10.1.2	Policy on the use of cryptographic controls	No
10.1.2	Key management	10.1.3	Key management	No
11	**Physical and environmental security**	**11**	**Physical and environmental security**	No
11.1	**Secure areas**	**11.1**	**Secure areas**	No
11.1.1	Physical security perimeter	11.1.2	Physical security perimeter	No
11.1.2	Physical entry controls	11.1.3	Physical entry controls	No
11.1.3	Securing offices, rooms and facilities	11.1.4	Securing offices, rooms and facilities	No
11.1.4	Protecting against external and environmental threats	11.1.5	Protecting against external and environmental threats	No
11.1.5	Working in secure areas	11.1.6	Working in secure areas	No
11.1.6	Delivery and loading areas	11.1.7	Delivery and loading areas	No
11.2	**Equipment**	**11.2**	**Equipment**	No
11.2.1	Equipment siting and protection	11.2.2	Equipment siting and protection	No
11.2.2	Supporting utilities	11.2.3	Supporting utilities	No
11.2.3	Cabling security	11.2.4	Cabling security	No
11.2.4	Equipment maintenance	11.2.5	Equipment maintenance	No
11.2.5	Removal of assets	11.2.6	Removal of assets	No
11.2.6	Security of equipment and assets off-premises	11.2.7	Security of equipment and assets off-premises	No
11.2.7	Secure disposal or re-use of equipment	11.2.8	Secure disposal or re-use of equipment	Yes
11.2.8	Unattended user equipment	11.2.9	Unattended user equipment	No
11.2.9	Clear desk and clear screen policy	11.2.10	Clear desk and clear screen policy	No
12	**Operations security**	**12**	**Operations security**	No
12.1	**Operational procedures and responsibilities**	**12.1**	**Operational procedures and responsibilities**	No
12.1.1	Documented operating procedures	12.1.2	Documented operating procedures	No
12.1.2	Change management	12.1.3	Change management	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

12.1.3	Capacity management	12.1.4	Capacity management	
12.1.4	Separation of development, testing and operational environments	12.1.5	Separation of development, testing and operational environments	Yes
12.2	**Protection from malware**	**12.2**	**Protection from malware**	No
12.2.1	Controls against malware	12.2.2	Controls against malware	No
12.3	**Backup**	**12.3**	**Backup**	No
12.3.1	Information backup	12.3.2	Information backup	Yes
12.4	**Logging and monitoring**	**12.4**	**Logging and monitoring**	No
12.4.1	Event logging	12.4.2	Event logging	Yes
12.4.2	Protection of log information	12.4.3	Protection of log information	Yes
12.4.3	Administrator and operator logs	12.4.4	Administrator and operator logs	Yes
12.4.4	Clock synchronization	12.4.5	Clock synchronization	No
12.5	**Control of operational software**	**12.5**	**Control of operational software**	No
12.5.1	Installation of software on operational systems	12.5.2	Installation of software on operational systems	No
12.6	**Technical vulnerability management**	**12.6**	**Technical vulnerability management**	No
12.6.1	Management of technical vulnerabilities	12.6.2	Management of technical vulnerabilities	No
12.6.2	Restrictions on software installation	12.6.3	Restrictions on software installation	No
12.7	**Information systems audit considerations**	**12.7**	**Information systems audit considerations**	No
12.7.1	Information systems audit controls	12.7.2	Information systems audit controls	No
13	**Communications security**	**13**	**Communications security**	No
13.1	**Network security management**	**13.1**	**Network security management**	No
13.1.1	Network controls	13.1.2	Network controls	No
13.1.2	Security of network services	13.1.3	Security of network services	No
13.1.3	Segregation in networks	13.1.4	Segregation in networks	No
13.2	**Information transfer**	**13.2**	**Information transfer**	No
13.2.1	Information transfer policies and procedures	13.2.2	Information transfer policies and procedures	Yes
13.2.2	Agreements on information transfer	13.2.3	Agreements on information transfer	No
13.2.3	Electronic messaging	13.2.4	Electronic messaging	No
13.2.4	Confidentiality or non-disclosure agreements	13.2.5	Confidentiality or non-disclosure agreements	Yes
14	**System acquisition, development and maintenance**	**14**	**System acquisition, development and maintenance**	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

14.1	**Security requirements of information systems**	**14.1**	**Security requirements of information systems**	No
14.1.1	Information security requirements analysis and specification	14.1.2	Information security requirements analysis and specification	Yes
14.1.2	Securing application services on public networks	14.1.3	Securing application services on public networks	No
14.1.3	Protecting application services transactions	14.1.4	Protecting application services transactions	No
14.2	**Security in development and support processes**	**14.2**	**Security in development and support process**	No
14.2.1	Secure development policy	14.2.2	Secure development policy	No
14.2.2	System change control procedures	14.2.3	System change control procedures	No
14.2.3	Technical review of applications after operating platform changes	14.2.4	Technical review of applications after operating platform changes	No
14.2.4	Restrictions on changes to software packages	14.2.5	Technical review of applications after operating platform changes	No
14.2.5	Secure system engineering principles	14.2.6	Secure system engineering principles	No
14.2.6	Secure development environment	14.2.7	Secure development environment	No
14.2.7	Outsourced development	14.2.8	Outsourced development	No
14.2.8	System security testing	14.2.9	System security testing	No
14.2.9	System acceptance testing	14.2.10	System acceptance testing	Yes
14.3	**Test data**	**14.3**	**Test data**	No
14.3.1	Protection of test data	14.3.2	Protection of test data	Yes
15	**Supplier relationships**	**15**	**Supplier relationships**	No
15.1	**Information security in supplier relationships**	**15.1**	**Information security in supplier relationships**	No
15.1.1	Information security policy for supplier relationships	15.1.2	Information security policy for supplier relationships	Yes
15.1.2	Addressing security within supplier agreements	15.1.3	Addressing security within supplier agreements	
15.1.3	Information and communication technology supply chain	15.1.4	Information and communication technology supply chain	No
15.2	**Supplier service delivery management**	**15.2**	**Supplier service delivery management**	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

15.2.1	Monitoring and review of supplier services	15.2.2	Monitoring and review of supplier services	No
15.2.2	Managing changes to supplier services	15.2.3	Managing changes to supplier services	No
16	**Information security incident management**	**16**	**Information security incident management**	No
16.1	**Management of information security incident management**	**16.1**	**Management of information security incident management**	No
16.1.1	Responsibilities and procedures	16.1.2	Responsibilities and procedures	Yes
16.1.2	Reporting information security events	16.1.3	Reporting information security events	Yes
16.1.3	Reporting information security weaknesses	16.1.4	Reporting information security weaknesses	No
16.1.4	Assessment of and decision on information security events	16.1.5	Assessment of and decision on information security events	No
16.1.5	Response to information security incidents	16.1.6	Response to information security incidents	No
16.1.6	Learning from information security incidents	16.1.7	Learning from information security incidents	No
16.1.7	Collection of evidence	16.1.8	Collection of evidence	No
17	**Information security aspects of business continuity management**	**17**	**Information security aspects of business continuity management**	No
17.1	**Information security conformity**	**17.1**	**Information security conformity**	No
17.1.1	Planning information security continuity	17.1.2	Planning information security continuity	No
17.1.2	Implementing information security continuity	17.1.3	Implementing information security continuity	No
17.1.3	Verify, review and evaluate information security continuity	17.1.4	Verify, review and evaluate information security continuity	No
17.2	**Redundancies**	**17.2**	**Redundancies**	No
17.2.1	Availability of information processing facilities	17.2.2	Availability of information processing facilities	No
18	**Compliance**	**18**	**Compliance**	No
18.1	**Compliance with legal and contractual requirements**	**18.1**	**Compliance with legal and contractual requirements**	No
18.1.1	Identification of applicable legislation and contractual requirements	18.1.2	Identification of applicable legislation and contractual requirements	Yes
18.1.2	Intellectual property rights	18.1.3	Intellectual property rights	No
18.1.3	Protection of records	18.1.4	Protection of records	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

18.1.4	Privacy and protection of personally identifiable information	18.1.5	Privacy and protection of personally identifiable information	No
18.1.5	Regulation of cryptographic controls	18.1.6	Regulation of cryptographic controls	No
18.2	**Information security reviews**	**18.2**	**Information security reviews**	No
18.2.1	Independent review of information security	18.2.2	Independent review of information security	Yes
18.2.2	Compliance with security policies and standards	18.2.3	Compliance with security policies and standards	No
18.2.3	Technical compliance review	18.2.4	Technical compliance review	No

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

Annex C – NPC MC 16-01 and ISO/IEC 29151

This table illustrates the relevant clauses of ISO/IEC 29151 to the NPC Memorandum Circular 16-01's requirements.

NPC Memorandum Circular 16-01	ISO/IEC 29151
Sec.4 General Obligations	5.1 **Management directions for information security**
Sec.5 Privacy Impact Assessment	A.11.2 Privacy impact assessment
Sec.6 Control Framework for Data Protection	5 Information security policies
Sec.7 General Rule on Storage of Personal Data	4.6 Lifecycle considerations
Sec.8 Encryption of Personal Data	10 Cryptography
Sec.9 Restricted Access	9.4.2 Information access restriction
Sec.10 Service Provider as Personal Information Processor	15 Supplier relationships
Sec.11 Audit	A.11.4 Privacy monitoring and auditing
Sec.12 Recommended Independent Verification or Certification	A.13 Privacy compliance
Sec.13 Archives	A.7 Use, retention and disclosure limitation
Sec.14 Access to or Modification of Databases	14.1 Restrictions on changes to software packages
Sec.15 Security Clearance	9 Access control
Sec.16 Contractors, Consultants, and Service Providers	15 Supplier relationships
Sec.17 Acceptable Use Policy	8.1.4 Acceptable use of assets
Sec. 18 Online Access to Personal Data.	8 Asset management
Sec.19 Local Copies of Personal Data Accessed Online	
Sec.20 Authorized Devices	8.3 Media handling
Sec.21 Remote Disconnection or Deletion	6.2 Mobile devices and teleworking
Sec.22 Paper-based filing system	8 Asset management
Sec.23 Personal Data Sharing Agreements	A.13 Privacy compliance
Sec.24 Emails	13 Communications security
Sec.25 Personal Productivity Software	8 Asset
Sec.26 Portable Media	7 Human resource security
Sec.27 Removable Physical Media	8 Asset Management
Sec.28 Fax Machines	
Sec.29 Transmittal	A.7 Use, retention and disclosure limitation
Sec.30 Archival Obligations	A.7 Use, retention and disclosure limitation
Sec.31 Procedures for Disposal of Personal Data	A.7 Use, retention and disclosure limitation
Sec.33 Data Breach Management	16 Information security incident management

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph

5F, Delegation Building, Philippine International Conference Center (PICC) Complex, Pasay City. Tel. no. +632 569 9623
URL: http://privacy.gov.ph Email Add: info@privacy.gov.ph