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. 2021-003

ISO/IEC 24760 – Information technology – Security techniques – A framework for identity management

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 24760-series for PICs and PIPs that carry out management of identity information in management systems.

Scope of the International Standard (IS)

These ISs provide definition of terms and core concepts of identity, identity management and their relationships. This is especially important to make decisions based on gathered

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

information, which will enable organizations to make identity-based decisions, which they may use to grant or deny access to applications or other organizational resources.

Requirements

ISO/IEC 24760-1:2019[1] "IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts"

1. Scope – This document defines terms for identity management and specifies core concepts of identity and identity management and their relationships.
   It is applicable to any information system that process identity information.

Below are the contents of the document:

2. Normative references: Refer to ISO/IEC 24760-2:2015, Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
3. Terms and definitions
4. Symbols and abbreviated terms
5. Identity
6. Attributes
7. Managing identity information
8. Identification
9. Authentication
10. Maintenance
11. Implementation aspects
12. Privacy

ISO/IEC 24760-2:2015[2], Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements

1. Scope – This document provides guidelines for the implementation of systems for the management of identity information and specifies requirements for the implementation and operation of a framework for identity management.
   ISO/IEC 24760-2:2015 is applicable to any information system where information relating to identity is processed or stored.

Below are the contents of the document:

2. Normative references
3. Terms and definitions
4. Symbols and abbreviated terms

[1] https://www.iso.org/standard/77582.html
[2] https://www.iso.org/standard/57915.html
The scopes are directly lifted from the IS documents, terms may be different from the DPA of 2012 but it has the similar meaning to the DPA terms. Refer to Annex A for the comparison of terms.

5. Reference Architecture
6. Requirements for the management of identity information

ISO/IEC 24760-3:2016[3] - Information technology – Security techniques – A framework for identity management – Part 3: Practice

1. Scope – This document provides guidance for the management of identity management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.
   It is applicable to an identity management system where identifies or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision-making using attributes of entities. practices for identity management can also be addressed in other standards.

Below are the contents of this document:

2. Normative references
3. Terms and definitions
4. Symbols and abbreviated terms
5. Mitigating identity related risk in managing identity information
6. Identity information and identifiers
7. Auditing identity and information usage
8. Control objectives and controls

[3] https://www.iso.org/standard/57916.html
The scopes are directly lifted from the IS documents, terms may be different from the DPA of 2012 but it has the similar meaning to the DPA terms. Refer to Annex A for the comparison of terms.

Benefits

For organizations to make identity-based decisions, the ISO/IEC 24760 series (a three-part standard) specifies a framework for the issuance, administration and use of data that serves to characterize individuals, organizations or information technology components, which operate on behalf of individuals or organizations. Proper management of identity information is crucial to protect privacy.

ISO/IEC 24760-1:2019 - IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts"

This international standard is part one out of three of the ISO/IEC 24760 multi-part standard. Its main goal is to specify terminology and concepts for identity management in order to promote a common understanding in the field of identity management.

ISO/IEC 24760-2:2015 -Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements

This international standard is part two out of three of the ISO/IEC 24760 multi-part standard. Its main goal is intended to provide a foundation for the implementation of other international standards related to identity information processing, such as:

- ISO/IEC 29100, Information technology – Security techniques – Privacy framework;
- ISO/IEC 29101, Information technology – Security techniques – Privacy reference architecture;
- ISO/IEC 29115, Information technology – Security techniques – Entity authentication assurance framework; and
- ISO/IEC 29146, Information technology – Security techniques – A framework for access management

ISO/IEC 24760-3:2016 - Information technology – Security techniques – A framework for identity management – Part 3: Practice

This international standard is part three out of three of the ISO/IEC 24760 multi-part standard. Its main goal is to specify fundamental concepts and operational structures of identity management with the purpose to realize information system management, so that information systems can meet business, contractual, regulatory and legal obligations. This last part of the ISO/IEC 24760 multipart standards aim to present practices for identity management that cover assurance in controlling identity information, use, controlling the access to identity information and other resources based on identity formation, and controlling objectives that should be implemented when establishing and maintaining an identity management system.

This part of ISO/IEC 24760 consists of the following parts:

- ISO/IEC 24760-1: Terminology and concepts;

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

- ISO/IEC 24760-2: Reference architecture and requirements; and
- ISO/IEC 24760-3: Practice

Like 24760-2, this is likewise intended to provide foundations for other identity management related International Standards including the following:

- ISO/IEC 29100, Information technology – Security techniques – Privacy framework;
- ISO/IEC 29101, Information technology – Security techniques – Privacy reference architecture;
- ISO/IEC 29115, Information technology – Security techniques – Entity authentication assurance framework; and
- ISO/IEC 29146, Information technology – Security techniques – A framework for access management

This series of standards would be beneficial to organizations for both public and private organizations in the country that manages identity information. Identity is often a requirement for authorization and authentication activities. These standards would help and serve as a basis for its proper management.

Guide for Adoption

The ISO/IEC 24760 series provide foundational terminologies, concepts, reference architecture and practical aspects of identity management. These International Standards are important for organizations who implement identity management systems, specifically, this enables access controls as a security measure to organization's systems and resources, which include but are not limited to implementing:

1) the need-to-know and least privilege principle;
2) Segregation of duties and responsibilities;
3) Privileged account management; and
4) Identity information lifecycle. Likewise, this is a welcome development for the government who operationalizes and maintain identification to their constituents.

These 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.

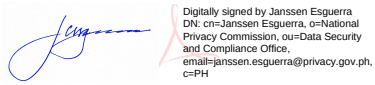
PICs and PIPs who adopt and implement these International Standards across their organizations shall harmonize and cross-reference equivalent terminologies in the DPA, its IRR and other relevant issuances of the National Privacy Commission (NPC). These IS does not amend the DPA, its IRR, and other relevant issuances of the NPC. In the event of a conflict

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

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.

Copies of the standards are 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.

Prepared By:

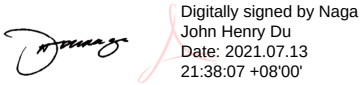


JANSSEN C. ESGUERRA
ITO I, DSTSD

Reviewed By:

KELVIN S. MAGTALAS
OIC-Chief, DSTSD

Recommending Approval:



ATTY. 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