**Public Key Infrastructure**

**(PKI) Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of Menara Organization and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from Menara Organization, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author/Editor** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**PURPOSE 4**

**SCOPE 4**

***POLICY* 4**

**ENFORCEMENT 7**

1. **PURPOSE**

This document defines the controls for implementing Public Key Infrastructure (PKI) within Organization Group and third parties that connects to Organization Group. Public Key Infrastructure (PKI) is the combination of software, encryption technologies, and services that enables the Group to ensure the security of business communications and transactions on the Internet, Intranet and Extranet. The objective of implementing PKI is to achieve privacy, confidentiality, data integrity and non-repudiation.

1. **SCOPE**

This document applies to all Organization Group employees, contractors, consultants, temporaries, and customers utilizing PKI to access the Organization Group’s network.

1. ***POLICY***
   1. **General**

PKIs integrate digital certificates, public-key cryptography, and certificate authorities into a total enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrolment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

* 1. **Certification Authority (CA)**
     + 1. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information.
       2. Organization Group should only accept 2 types of CA which are Organization Internal CA and Trusted 3rd Parties CA. Trusted 3rd Parties CA is refer to 3rd Parties CA that recognized by the local court of law.
       3. The Trusted 3rd Parties CA makes its own public key readily available through print publicity or on the Internet. Organization Internal CA should only distribute its own public key among Organization Group.
       4. The roles of a CA are as below:-
          1. Issuing certificate
          2. Managing certificate
          3. Renew certificate
          4. Revoke certificate
       5. Organization Internal CA is the highest-level active certification entities within Organization Group and act as its own roots. The Organization Internal CA issues, suspend and revoke all Organization internal certificates.
       6. Organization root key shall be securely generated. The private key must be kept secured by using a trustworthy system, and take necessary precautions to prevent its loss, disclosure, modification or unauthorized use.
       7. Both CAs should have operational controls and record keeping for certificate issuance.
  2. **Digital Certificate**
     + 1. A Digital Certificate is issued by a Certification Authority to confirm the subscriber identity to others. Once issued, the certificate can be used for variety of tasks; such as protecting email data, performing digital signing for internet transaction or providing a secure connection to another computer.
       2. There are 4 types of digital certificates.
          1. Email certificate.
          2. User certificate.
          3. Server certificate.
          4. CA certificate (also call as root certificate).
       3. All certificates must have a validity period. The recommended validity period for all subscriber certificates is 1 year except for the CA certificates, which validity period can be more than 1 year.
       4. Subscriber’s key pair must be generated securely. The subscriber’s public key and subscriber’s information will submit to the CA as part of the Certificate Signing Request (CSR). The CA will only sign and issue the Digital Certificate after the validation and verification are done.
       5. Validation, verification and authentication have to be done on the subscriber before a digital certificate can be issued.
       6. Certificates that issued by Organization Internal CA are strictly for internal use only. It is only allowed to be used for encryption and server authentication.
       7. Notice prior to certificate expiration. Key manager should make a reasonable effort to notify the system administrator/owner, in email of the impending expiration of the certificate. Please refer to PKI Procedure for the roles and responsibilities of the Key manager.
       8. A certificate shall be considered to be unreliable, and shall need to be suspended or revoked if there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate’s subject.
       9. Certificates that issued by Trusted 3rd Parties CA can be widely adopted for internal and external usage. The usage of those certificates will depend on the Certificate Practice Statement (CPS) that defined by the Trusted 3rd Parties CA.
  3. **Encryption**
     + 1. Certificates issued by Organization Internal CA are used for encryption between Organization Group. The encryption technologies used should be proven and complies with accepted industrial standard. E.g. S/MIME, SSL/TLS session, VPN and IPSEC.
       2. Encryption to 3rd party entity should use a digital certificate that issued by a Trusted 3rd Parties CA.
       3. All encryption connections must have strong encryption strength. The key length requirements will be reviewed annually and upgraded as technology allows. Refer to Organization Acceptable Encryption ***Policy*** for more details.
  4. **Digital Signature**
     + 1. Organization internal certificates are not allowed to do digital signing for non-repudiation purposes business transaction. This is due to certificate that issued by Organization Internal CA is not recognized by the local court of law.
       2. All digital signing on internet transactions must use certificates that issued by Trusted 3rd Parties CA.
       3. Certificate issued by Organization Internal CA can only be used for email digital signature (S/MIME) in Organization Group only.
       4. Trusted 3rd Parties CA digital certificate must be used for any digital signature (S/MIME) communication to the world.
       5. Digital certificate should be verified against Certificate Revocation List (CRL) when used for any digital signing.
  5. **Authentication**
     + 1. There are 2 types of authentication
          1. Server authentication.
          2. User authentication.
       2. Organization Internal CA can only authenticate and issue a server certificate to the internal servers and accessed by Organization internal users.
       3. For servers that are accessed by public users, the server certificate has to be issued by Trusted 3rd Parties CA. However, server certificate issued by Trusted 3rd Parties CA may be used for internal server.
       4. Servers with valid domain names have to be authenticated before a server certificate can be issued.
       5. Certificate issued by Trusted 3rd Parties CA can be used for any user authentication on all systems.
       6. Certificate issued by Organization Internal CA can only be used for user authentication on Organization internal system.
       7. Digital certificate should be verified against Certificate Revocation List (CRL) when doing authentication.
  6. **Certification Revocation List (CRL)**
     + 1. CRL contains a time stamped list of revoked certificates that a Certification Authority (CA) signs and makes available to PKI users in a public repository. A CRL identifies each revoked certificate by its certificate serial number.
       2. All digital certificates must be revoked and publish in the CRL if the certificate have been compromised or suspected to be compromised. This does not apply to rudimentary level of certificate.
       3. The serial number of the compromised digital certificate should be published in the CRL within 24 hours.
  7. **Key Recovery**
     + 1. Key recovery is only allowed on encryption key but not the signing key.

1. **ENFORCEMENT**

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. ***Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.***
  2. ***Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.***