INFORMATION TECHNOLOGY INSTRUCTIONS

March 2015

Ministry of Resource Development
and Information Technology

CONTENT

CHAPTER I: INTRODUCTION

1. Objective

The Information Technology (IT) Instructions in this context serve as guidelines intended to meet the minimum requirements to support the Electronic Government Activities Enactment (EGAE) 2014 in facilitating electronic transactions.

2. Background

2.1. The EGAE 2014 provides the legal framework for efficient and secure electronic Government services. The purpose of this Enactment is to enable and facilitate electronic dealings by the State Government Agencies with the public in a uniform manner.

2.2. The EGAE 2014 applies once the Agencies are ready to handle electronic dealings and does not grant any additional legal rights or change any substantive law.

2.3. Under Section 9 of the Enactment, the Minister responsible may issue IT Instructions that will be a minimum requirement for the Agencies in undertaking electronic transactions. In this regard, when Agencies embark on any electronic-related initiative, Agencies can opt to use the IT Instructions as the guidelines for the related areas. As such, the Agencies should designate the relevant Enactment under the EGAE 2014 and subsequently, conform to the guidelines stipulated in the instructions for the designated areas.

3. Scope

3.1. This document consists of IT Instructions which encompasses the following areas:

3.1.1. information technology standards

3.1.2. the criteria for electronic signatures and electronic seals as appropriate for the purpose for which they are used

3.1.3. time recording, acknowledgement of receipt of electronic documents or messages

3.1.4. security measures against unauthorised access, unauthorised modification, denial of service and repudiation

3.1.5. disaster recovery procedures

3.1.6. accessibility rules for electronic Government services and electronic forms

3.1.7. management and maintenance of electronic documents

3.1.8. procedures related to data entry and verification of messages; and

3.1.9. guidelines for payment and receipt of money

3.2. The areas above are incorporated in the various chapters as follows:

3.2.1. Chapter II: Application System

3.2.2. Chapter III: Information Communication Technology (ICT) Security Requirements; and

3.2.3. Chapter IV: Electronic Records Management

4. Application

4.1. IT Instructions is applicable to all State Government Agencies (herein after shall be referred to as “Agencies”).

4.2. This document shall be reviewed subject to changes with regards to:

4.2.1. technology

4.2.2. statutory and regulatory; and

4.2.3. stakeholders direction

5. Responsibilities of Agencies

Agencies which undertake or in the process of undertaking electronic transactions need to satisfy the minimum requirements of the IT Instructions where relevant.

CHAPTER II: APPLICATION SYSTEM

6. Overview

Applications installed and used within Agencies comprise a mixture of commercially and internally developed applications.

7. Objective

This chapter provides guidelines for minimum requirements on application systems for use by agencies responsible for developing, implementing or maintaining these applications.

8. Scope

8.1. The scope of this chapter covers the following areas:

8.1.1. Accessibility

(a) Multi-Channel

(b) Open Standards

(c) Interoperability; and

(d) Special Needs Community

8.1.2. Open Source Software

8.1.3. Software Quality, Testing and Audit

8.1.4. Data Entry, Validation and Verification

8.1.5. Time Recording and Acknowledgement of Receipt

8.1.6. Audit Trails; and

8.1.7. Payment and Receipt of Money

(a) General Instructions

(b) Payment; and

(c) Receipt

8.2. The areas above need to take into consideration the changes in technology and its impending trends, specifically to minimise impact and ensure stability and to prevent any major changes or modification to the requirements of the application systems employed.

9. Accessibility

9.1. The accessibility aspect of application systems will be described in terms of multi-channel, open standards, interoperability and special needs community.

9.1.1. Multi-Channel

Agencies are encouraged to provide services to the public through multiple electronic channels. The channels selected have to meet public/customer needs and requirements. Any customisation to the channels shall be made in this regard. Agencies need to observe the following with respect to multi-channel delivery:

(a) Multi-channel delivery should relate to the provision of Government services through Multimedia Messaging Service (MMS) or other electronic channels (e.g., Smart Phone, Tablet, Mobile Device, Telephone, Fax and Kiosk); messaging service (e.g., Short Messaging Service (SMS), e-mail, Internet and Interactive Voice Response); and conventional channels (e.g., meetings and counters);

(b) Agencies should decide on a mix of channels, where appropriate, to ensure customer accessibility. The mix of channels should be cost-effective from the perspective of both Agencies and customers;

(c) Agencies should identify their customers, their service requirements and preferences for particular channels;

(d) Agencies should use different criteria to segment their customers based on both needs and preferences. Customer segmentation allows for customers to be divided into manageable segments that have distinct characteristics. The identification of these characteristics enables the needs of a particular customer set to be determined and services tailored to meet those needs. Various criteria can be used to segment the customer markets such as geographic (e.g., region, city size), demographic (e.g., age, gender, income, occupation), psychographic (e.g., lifestyle, personality), etc.; and

(e) Agencies should identify barriers that may affect certain groups in their access to electronic channels. If a particular customer segment (e.g., the older aged groups) is unable to access or not well-versed with the usage of computers or related online technologies, other channels should be identified for this customer segment to facilitate access to the services provided.

9.1.2. Open Standards

The electronic delivery services should be based on Open Standards developed in an open and transparent manner with industry participation. It is non-proprietary and commonly owned, has open specification access encompassing free access to all interface specifications. The Open Standards specification is technology neutral.

9.1.3. Interoperability

Agencies should develop application based on Open Standards to ensure interoperability and accessibility.

9.1.4. Special Needs Community

The services rendered should cater for the special needs community, such as the physically challenged (e.g., the height and the area surrounding the kiosks should be convenient for wheelchair users) and senior citizens (e.g., fonts on the kiosk monitor should be of appropriate size).

10. Open Source Software

10.1. The State Government of Sabah encourages the adoption of Open Source Software (OSS) for developing application systems.

10.2. The implementation of OSS should be based on several key considerations such as:

10.2.1. fit for purpose in terms of functionality as well as technology platform

10.2.2. least disruptive to the current business operations; and

10.2.3. must have the capabilities to co-exist with other legacy systems/solutions

11. Software Quality, Testing and Audit

11.1. Emphasis must be given to the quality of the application as it reflects on the overall quality of the product. In the context of the EGAE, it reflects on the quality of service the application provides and functions in accordance to the requirements and standards set out within.

11.2. Applications developed must be well documented in accordance to software engineering best practices. The documentations shall include:

11.2.1. Software and System Requirements

11.2.2. Software and System Design

11.2.3. Software and System Test Design

11.2.4. Quality Control Design

11.3. The overall aspects of software quality of the application should conform to the product quality model as prescribed under the ISO/IEC 25010 – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models.

11.4. The primary purpose of software testing is quality assurance, verification and validation, reliability and design defects. To assure that the application is of quality and fit for production, An application must undergo an independent software testing process to assure of its quality and fit for production status. Software testing must be broadly deployed in every phase of the application software development cycle. Software testing activities must be made integral to the Quality Control Design of the application.

11.5. For the remainder of the application production lifetime, it is essential for the application to undergo an audit process to ensure that quality remains consistent and also to identify opportunities for improvement. Therefore, the agency must establish regular audits on their applications.

12. Data Entry, Validation and Verification

12.1. Procedures relating to data entry, validation and verification should ensure that electronic forms are designed to allow correction of errors by the user filling in the forms prior to submission of the forms (e.g., system prompts a dialogue box requesting a confirmation before the user submits the form).

12.2. Data entered into application system must be validated to ensure it is correct and appropriate. Input checks must be implemented to detect the following errors where appropriate, for example:

12.2.1. out of range values

12.2.2. missing or incomplete data

12.2.3. invalid characters in data fields

12.2.4. exceeding limits

12.2.5. unauthorised data (e.g., fields for approval of application can only be updated by authorised personnel); and

12.2.6. inconsistent data

13. Time Recording and Acknowledgement of Receipt

13.1. Systems for recording date and time and acknowledgement of receipt must be in place to avoid disputes on when a document was received and the time it was received. This is particularly crucial where documents or information must be delivered by a particular date and time.

13.2. Procedure to check and correct the accuracy of clock must be established such as using the Network Time Protocol (NTP) which is designed to synchronise the clocks of computer systems (www.ntp.org). Real time clock of communication devices must be set in accordance with the *Malaysian Standard Time Act 1981*.

13.3. Time recording and acknowledgement of receipt shall take into account the front-end and backend components, that is those that correspond to the submission of forms and processing of transactions:

13.3.1. Front-End: Submission of Forms

Acknowledgement of submission using server time is required regardless of the type of transactions or processing that needs to be done. The process should include but not limited to the following:

(a) data/document entering the server

(b) acknowledgement of receipt; and

(c) referencing of submission of forms

13.3.2. Back-End: Transactions Processing

Detailed recording of receipt is required using server time. The process should include but not limited to the following:

(a) data/document entering the server

(b) updating of database

(c) acknowledgement of receipt after successful updates of database; and

(d) referencing of receipts

13.4. There is a vital need to have some kind of notification mechanism for any failures (e.g., network failure).

14. Audit Trails

14.1. Audit trails are records of activities used to provide a means of recording events and establishing accountability. It is essential to ensure the accuracy of audit logs that are required for investigations or as evidence in legal or disciplinary cases.

14.2. Several types of logs must be captured and kept, namely system log, network log, server log and transactions log. The type of log and duration of archiving the logs should be referred to any relevant Acts (e.g., *State Archives Enactment 1980* and *Sabah State Records and Archives Enactment 2007*), otherwise, the minimum duration for archiving should be one (1) year relative to the previous year.

14.3. The following must be observed in relation to audit trails:

14.3.1. All systems must be auditable.

14.3.2. Changes to data must be recorded in chronological order and in sufficient detail. A complete history of transactions must be recorded and preserved for each session involving access to classified information and other sensitive information as per the *Arahan Keselamatan* to permit an audit of the system. In this respect, the following audit trails must be established and preserved:

(a) system operation start-up and shut-down sessions; and

(b) transaction histories with a minimum log of the following information:

(i) all types of transactions

(ii) date and time of activity

(iii) user identification

(iv) sign-on and sign-off activity; and

(v) sensitive display transactions (e.g., access to classified reports, usage of sensitive user identification)

14.3.3. The purchase of any equipment or system pertaining to the processing and recording of classified, confidential or sensitive information shall refer to and comply with paragraphs 28 and 29 of the *Arahan Keselamatan* by the Office of the Chief Government Security Officer.

14.3.4. An analysis of transaction histories for the purpose of detecting variances from the norm must be conducted once a month to:

(a) detect access failures

(b) detect abnormal use such as unusual login time, frequency and length of accesses

(c) monitor privileged access

(d) track selected transactions; and

(e) observe the use of sensitive resources such as blank cheques, passports, examination certificates, birth certificates, etc.

14.4. The audit log must be tamper-proof and its integrity is beyond doubt (refer Chapter III: ICT Security Requirements).

15. Payment and Receipt of Money

15.1. The applications utilised for payment and receipt of money must be equipped with the appropriate approval procedures, compliance requirements, work processes, security features, storage and audit trail capabilities. The instructions for these features are described in a general manner, followed by more specific guidelines on payment and receipt respectively.

15.1.1. <u>General Instructions</u>

(a) The development and modification of financial systems, such as systems relating to payment and receipt of money must obtain prior written approval from the State Treasury Department.

(b) The development and operation of financial systems must comply with the requirements and provisions governed by the *Treasury Instructions*.

(c) There must be clear written procedures on the work processes required to be followed by users of the system. Users must keep all supporting documents used as a basis to input data.

(d) All data input and generated by the system must be kept intact and secured so that the data can be retrieved in any form specified when the need arises.

(e) Data must be kept in the system for a minimum period in accordance to the duration stipulated by the *Treasury Instructions*.

(f) The system must keep a detailed audit trail of all transactions.

15.1.2. Payment

(a) For every payment that has been made electronically, the system must ensure that the payee is notified. Sufficient details on the purpose of payment must be clearly stated in the notification. The system must also provide a facility to allow payees to enquire about their payment status.

(b) There must be sufficient control to allow only authorised persons to update information in the database. Sufficient control must exist in the system to ensure that payments made electronically are received by the intended recipients.

(c) Transmissions of data to banking institutions for payment purposes must be properly and adequately protected from any form of tampering (please refer Chapter III: ICT Security Requirements).

(d) The roles and limitations of access for each authorised personnel in the payment process must be clearly stated and controlled in the system. The system should be able to identify clearly the personnel responsible for any financial transaction.

15.1.3. Receipt

(a) Receipt of money can be of any mode that is approved by the Ministry of Finance. The mode of collection must be indicated in the system and in all issued receipts.

(b) If Agencies are authorised to collect in a currency other than the local currency, the system should record:

(i) the exchange rate

(ii) the date of the exchange rate; and

(iii) the equivalent amount in local currency

(c) The system must be able to identify or relate any receipt to the correct collection record.

(d) Where any law requires any payment to be made, the requirement of such law is fulfilled if such payment is made by electronic channels (e.g., kiosks or virtual receipts such as SMS) and complies with any conditions imposed by the Government.

(e) The system must ensure that information on the payment is made accessible as and when required by the public.

(f) Where any law requires any issuance of receipts of payment, the requirement of such law is fulfilled by the issuance of receipt by electronic means if the receipt is accessible, legible and can be used for subsequent reference.

CHAPTER IV: SECURITY REQUIREMENTS

16. Overview

16.1. Agencies ICT processing systems are not immune to ICT security threats. The main threats are unauthorised access, modification, disclosure and either deliberate or accidental destruction of information. These threats may originate from a wide range of sources, such as malicious codes, fraud, theft, espionage, sabotage and intrusion. The impact of these threats can be mitigated by establishing and monitoring a suitable set of controls, including policies, processes, procedures, organisational structures, software and hardware functions in conjunction with business management processes. Dependence on information system for public service delivery and the interconnection of public/private sector networks for information sharing services require Agencies to be constantly vigilant against threats, risks, vulnerabilities and exposures.

16.2. Agencies should protect ICT systems under its ownership or control against risks, threats, vulnerabilities or exposures by mitigating its effects cost effectively to ensure service delivery continuity and minimise service disruption.

16.3. Departmental Heads should be responsible to ensure adequate and appropriate security of ICT assets under their care and/or control as per *Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan* and *Dasar Keselamatan ICT Sektor Awam Negeri Sabah*.

17. Objective

This chapter provides guidelines for minimum requirements on ICT security to protect the confidentiality, integrity, availability, authenticity and non-repudiation of ICT assets.

18. Scope

18.1. The scope of this chapter covers Agencies ICT security planning and implementation with regards to the following areas:

18.1.1. Characteristics of Information Security

18.1.2. Risk Assessment and Treatment Plan; and

18.1.3. ICT Security Domains

19. Characteristics of Information Security

19.1. Main characteristics of information security are as follows:

19.1.1. Confidentiality

19.1.2. Integrity

19.1.3. Availability

19.1.4. Authenticity; and

19.1.5. Non-Repudiation

19.2. Details of each characteristics of information security are as follows:

19.2.1. Confidentiality

(a) Confidentiality means preserving authorised restrictions on information access and disclosure. A loss of confidentiality is the unauthorised disclosure of information.

(b) All classified information should be encrypted during storage and transmission using recommended industry standard encryption algorithms that comply with the *Digital Signature Act 1997 (Act 562).*

(c) All private keys should be secured and kept confidential. A report is to be made immediately when private keys are lost or destroyed.

(d) All cryptographic keys should be stored in a secure and tamper proof Hardware Security Module (HSM).

(e) Agencies should secure transmissions end–to–end and to protect traffic from eavesdropping, connection hijacking, and other network-level attack by making use of Secure Sockets Layer (SSL), Secure Shell (SSH) and HSM protocols of current versions.

(f) All HSMs should comply with the minimum Federal Information Processing Standard (FIPS) 140-2 level three (3) or equivalent.

19.2.2. Integrity

(a) Integrity means the guard against improper information modification and destruction, errors and omissions. A loss of integrity is the unauthorised disclosure and/or modification of information.

(b) Agencies should implement integrity checks such as hash total to prevent errors and omissions to preserve integrity.

(c) Comprehensive built-in checks should be incorporated within the security sub-system to ensure integrity and completeness of all data sent to/received from external systems/applications.

(d) Application systems and security infrastructure implemented should be protected against external and internal network attacks.

19.2.3. Availability

(a) Availability means to ensure on demand access to data and resources to authorised individuals.

(b) Protection mechanisms should be in place to protect against threats that could affect the availability of network systems and information.

(c) Single point of failure should be avoided.

(d) Backup measures should be taken and redundancy mechanisms in place when necessary. Backup devices must be made available to quickly replace critical systems when there is a disruption.

(e) Skilled personnel should be made available to bring the system back online immediately.

(f) Only necessary services and ports should be made available.

(g) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) should be in place to monitor network traffic and host activities.

19.2.4. Authenticity

(a) Authenticity means the assurance that a particular subject (user, program or process) has been identified and verified with a set of credential against information that has been previously stored to ensure that the subject is the entity that it claims to be.

(b) For a subject to be able to access a resource, it has first to prove who it claims to be, has the required credentials, and has been given the authority to perform the requested actions.

(c) All activities performed on Agencies ICT system resources should be recorded for the purpose of detection and accountability.

(d) Agencies should properly evaluate the technique used for identification and authentication to determine the right mechanism to suit the environment.

(e) Agencies should implement two-factor authentication.

19.2.5. Non-Repudiation

(a) Non-repudiation means the provision for proof of the integrity and origin of data in such a way that the integrity and origin can be verified from successfully denying involvement in a previous action. Non-repudiation is achieved cryptographically by the use of a digital signature.

(b) Digital signature should be used to achieve non-repudiation. Digital signature should comply with the requirements of the *Digital Signature Act 1997 (Act 562)*.

20. Risk Assessment and Treatment Plan

20.1. Risk assessment will assist Agencies to identify risks, threats, vulnerabilities and exposures. Once risks, threats, vulnerabilities and exposures have been identified and decisions for the treatment made, appropriate controls should be selected and implemented to ensure mitigation to an acceptable level.

20.2. The standard methodology based on *Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam* should be employed to conduct risk assessment. Agencies are required to conduct The *Malaysian Public Sector Information Security High Level Risk Assessment (HiLRA)* and/or The *Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)* in assessing their risks.

20.3. Risk assessment should be performed at least once a year or as and when there are changes in security requirements or changes in Agencies ICT environment.

21. ICT Security Domains

21.1. There are eleven (11) ICT Security domains as follows:

21.1.1. ICT Security Policy

(a) The ICT Security Policy is the most critical element of Agencies ICT security program. This policy identifies overall direction of Agencies ICT security and as a guide for the development of more specific rules to address specific situations.

(b) Agencies should acknowledge its obligation to ensure appropriate security for all ICT assets under its ownership. This is implemented by having a written ICT Security Policy that serve to assist in identifying what needs to be protected and to inform Agencies personnel, activities that are allowed or disallowed. The policy should define common rules to be abided by Agencies personnel. The policy should address the need for a total enforcement of controls and measures to safeguard Agencies ICT assets.

(c) Agencies should develop their ICT Security Policy based on their respective environment.

(d) The ICT Security Policy should be approved by Agencies top management, published and communicated to all Agencies personnel and to any related external party if required, with care not to disclose sensitive information.

(e) The ICT Security Policy should be relevant, disseminated across Agencies, made aware, enforced and monitored for compliance.

(f) All ICT security-related management activities (e.g., user authentication, application privileges and ICT security policy management) should be administered by a single unified administration.

(g) The ICT Security Policy should have an owner responsible to develop, evaluate and review and evaluate the policy.

(h) The ICT Security Policy should be reviewed at planned intervals or when there is significant change to the organisation to ensure the policy remains sustainable, relevant and efficient.

(i) Policy reviewed should be recorded. The revised policy document should be approved by top management and again made known to the personnel.

21.1.2. ICT Security Management Structure

(a) Agencies should recognise that the organisational structure for ICT security is vital to initiate and control the implementation of ICT security.

(b) A management group should be in place to ensure support for ICT security initiatives.

(c) A senior officer should be appointed as an ICT Security Officer (ICTSO) to manage the overall ICT security program.

(d) The ICTSO should ensure security activities are executed in compliance with Agencies ICT Security Policy.

21.1.3. Asset Management

(a) Public Sector ICT assets should be protected at all times against unauthorised access and disclosure.

(b) ICT assets should be clearly identified and properly managed to maintain its confidentiality, integrity and availability. ICT assets include both tangible and intangible assets such as licence, patent, brand, trademark, copyright and business methodology as per *Section 3 Financial Procedure Act 1957 (revised 1972).*

(c) All ICT assets should be accounted, have an inventory record and owner.

(d) The ICT asset inventory should include all information necessary to recover from a disaster, including type of asset, format, location, backup information, license information and a business value.

(e) Information classification should follow the *Arahan Keselamatan* and levels of protection required should be agreed upon and documented for every asset.

(f) Agencies personnel, contractors and third party users accessing Agencies ICT assets should be made aware of the limits of their use and be made accountable for the assets they use.

21.1.4. Human Resource Security

(a) For any Agencies, the personnel are its most important asset. Through proper planning of acculturation, personnel can contribute a great deal to achieving the mission and vision of the Agencies. Personnel play a crucial role in supporting Agencies ICT security programmes. Equipped with proper training, most personnel can be depended upon to identify anomalies and deviations from good security practices, which can then be the basis for remedial actions.

(b) Agencies should inculcate the users that ICT resources they are privy to, belong to the Government including data, stated information or information that is derived. The Government being the owner, reserves the right to monitor activities of users accessing its ICT resources to detect misuse or usage of ICT resources other than the purpose for which they were intended for.

(c) All users are accountable for their actions when accessing Public Sector ICT assets. This accountability has to be made clear to all users.

(d) All ICT information system should have the capability to record and detect user actions.

(e) Agencies personnel, contractors and third party users should be adequately screened in accordance to the relevant laws, regulations, ethics and proportional to the classification of the information to be accessed and the related risks involved.

(f) Agencies personnel, contractors and third party users should be made aware of their security roles and responsibilities as defined in the Agencies ICT Security Policy.

(g) Agencies personnel and if required, contractors and third party users should be given training, awareness programme and regular updates with regard to Agencies policies and procedures related to their job function.

(h) Agencies should manage exit, termination, change of roles and responsibilities of their personnel, contractors and third party users to ensure that all Agencies equipment, software and documents are returned and access rights revoked.

21.1.5. Physical and Environmental Security

(a) This paragraph should be read together with *Arahan Keselamatan* issued by the Office of the Chief Government Security Office.

(b) To prevent unauthorised access, damage and interference, physical protection should commensurate with the identified risk and be based on the principle of defence-in-depth.

(c) Critical or sensitive ICT facilities should be housed in a secure area, away from public view, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

(d) Secure areas should be protected by appropriate entry controls to ensure only authorised personnel are allowed access.

(e) Limit physical access to personnel and/or maintenance crew who are necessary for the operation of the ICT system.

(f) Access points such as delivery and loading areas and other points where unauthorised persons may enter the premise, should be controlled and if possible, isolated from ICT processing facilities to avoid unauthorised access.

(g) Physical protection should be in place to protect against damage from fire, flood, pests, explosion, civil unrest and other forms of natural or man-made disaster.

(h) Proposals related to buildings, acquisition, lease, renovation, purchase of Government and private buildings for housing ICT processing facilities should be referred to the Chief Government Security Officer (CGSO).

(i) Agencies supporting utilities equipment should be protected against power failures and other disruptions.

(j) Agencies should consider multiple power feeds to avoid a single point of failure.

(k) Agencies should ensure that power and telecommunications cabling carrying data or supporting information services are protected from interception or damage.

(l) Agencies should properly maintain all equipment to ensure continued availability and integrity.

(m) Agencies should obtain prior authorisation for all equipment, information or software before taken off-site.

(n) All equipment containing storage media should be checked to ensure that all sensitive data or licensed software has been transferred and/or securely deleted prior to disposal of the equipment.

21.1.6. Communications and Operations Management

(a) The management of communications and operations is vital to ensure secure and correct operation of ICT facilities. Agencies should establish communications and operations management by developing appropriate operating procedures to prevent unauthorised disclosure, modification, removal or destruction of assets and interruption to business activities.

(b) Agencies should ensure operating procedures are documented, maintained and made available to all users.

(c) Agencies should implement segregation of duties and assignment of minimum access rights to users to reduce the risk of negligent or deliberate misuse of systems.

(d) Agencies should control any changes to ICT facilities and systems.

(e) Agencies should separate the development, test and operational facilities to reduce the risks of unauthorised access or changes to the operational system.

(f) Agencies should be aware that ultimately they are responsible for information processed by an outsourced party. Services, reports and records provided by an outsourced party should be regularly monitored, reviewed and audited. Appropriate action should be taken when deficiencies in the service delivery are observed.

(g) Agencies should monitor, tune and project future capacity requirements for the use of resources to ensure the required system performance.

(h) Agencies should ensure that criteria and requirements for new system acceptance are clearly defined, agreed, documented and tested prior to acceptance. New information systems, upgrades and new versions should be tested and obtain formal acceptance before migrating into production. For major developments, users and operations personnel should be consulted at all stages of the development process to ensure operational efficiency of the proposed system design.

(i) Agencies should implement detection, prevention, recovery controls and user awareness programmes to protect ICT processing facilities and systems against malicious code. Usage of two (2) or more software products protecting against malicious code from different vendors can help improve the effectiveness of malicious code protection.

(j) Backup

(i) Backup is required to maintain the integrity and availability of information and ICT processing facilities. Standard Operating Procedures (SOP) should be established to provide guidance for doing backup and restore. This would involve all important files, data, application programs and documentation.

(ii) Backup files should be properly and clearly labelled to prevent accidental overwrite.

(iii) Access control to backup files should be restricted to authorised personnel with proper auditing record.

(iv) Backup should be performed on a daily, weekly, monthly and yearly basis. The frequency of backup depends on the criticality of the information.

(v) Agencies should have at least three (3) backup copies. Backup media should be securely stored and kept off-site. Access to the secured storage location should be strictly controlled against unauthorised access.

(vi) Agencies should test backup/restore procedures and backup media at least once a year.

(vii) Agencies should keep at least three (3) generations of backup.

(k) Audit Trails, Alerts and Reports

(i) Audit trail should be provided when:

a. critical information is accessed such as privileged information, changes to user profile and access to log files;

b. network services are accessed such as data packet verification, network applications, wireless Internet Protocol (IP); and

c. special privileges or authorities are used such as security administration instructions, emergency user identifications, supervisory functions and overrides of normal processing flow.

(ii) Audit trails of all events and critical activities should be centrally logged and integrity protected from accidental or intentional changes.

(iii) The audit logs should contain sufficient information details (e.g., user identity, specific transaction or program executed, functions, resources and information used or changed, date/time of access, details of changes, status of the request).

(iv) Comprehensive audit reports of user and security administration activities should be provided.

(v) Audit trails should be kept for a period as recommended by the *State Archives Enactment 1980* and *Sabah State Records and Archives Enactment 2007.*

21.1.7. Access Control

(a) Access to information, processes and ICT processing facilities should be controlled on the basis of roles and security requirements. Access control rules should take into account of policies for authorisation and information dissemination.

(b) All access to ICT assets should be defined and documented through a user registration procedure and controlled based on:

(i) need to know principle

(ii) roles

(iii) minimum access rights; and

(iv) separation of duties

(c) All privileges and access rights should be reviewed periodically. Privileged access should be restricted and monitored daily by the ICTSO.

(d) Access activities should be monitored daily to detect unusual activity such as repeated invalid access attempts that may threaten the integrity, confidentiality or availability of the system.

(e) Every user should be identified by a unique user identification associated only with that user and should be authenticated prior to gaining access to the information resource.

(f) The application security should support the following authentication methods:

  (i) normal identification and passwords; and/or

  (ii) certificate-based Public Key Infrastructure (PKI) authentication

(g) Identifications, passwords and authentication information should be kept confidential.

(h) Application security should have the following features:

  (i) Automatic logoff after a configurable period of inactivity

  (ii) Automatic re-authentication of active users after a pre-defined period

  (iii) Force logoff of users and revoke immediately all privileges of users who have been re-assigned, transferred or terminated

  (iv) Disallow concurrent login sessions for each user ID

  (v) Uniquely create user ID within the system

  (vi) Disable user and security administration accounts after a maximum number of three (3) failed login attempts

  (vii) Suspend user privileges after 30 days (configurable) of non-use and deleted after 30 days (configurable) of suspension

  (viii) Passwords should not be displayed on input, reports or other media and should not be hard-coded

  (ix) Enforce password change on initial login or login after password resets

(x) Enforce a change of password after 90 days or after a reasonable duration subject to policy review

(xi) Enforce minimum password length of 8 characters with a combination of alphabets, numbers and special characters

(xii) Prevent the re-use of a minimum of four (4) recently used passwords

(xiii) Passwords must be different from the user IDs

(xiv) Set time limit for authentication to two (2) minutes (configurable) upon which, the session is terminated; and

(xv) Display the date and time of the user's last successful and unsuccessful login

(i) ICTSO should be able to dynamically select authentication method for each application without the need to refer to the application source code.

(j) No automatic right of access will be granted to individuals regardless of their security vetting. In all instances of information exposure, the need to know principle must prevail.

(k) A clear desk or clear screen policy should be applied to all information storage media and ICT processing facilities.

(l) Agencies should consider:

(i) restricting access to Agencies operating system to authorised users only

(ii) using a secure login procedure; and

(iii) applying connection time controls for sensitive computer applications especially from high risk locations

(m) Agencies should restrict logical access to application software and information to authorised users. A dedicated computing environment should be provided for sensitive systems.

21.1.8. ICT Systems Acquisition, Development and Maintenance

(a) ICT system comprises hardware, network infrastructure, software including operating systems, user applications and off-the-shelf products and services. Security requirements should be identified, agreed and documented during the project requirements phase prior to the development and implementation of ICT System.

(b) Data input to applications should be validated to ensure that data is correct and appropriate.

(c) Applications should be incorporated with validation checks to detect any corruption of information resulting from processing errors or deliberate acts.

(d) Output derived from application system should be validated to ensure that the information is correct.

(e) A procedure to control the installation of software on operational systems should be in place.

(f) The implementation of changes should be controlled by the use of formal change control procedures.

(g) Test data should be selected carefully, protected and controlled.

(h) Agencies should practice testing of new software including patches, service packs and other updates, in an environment separated from the development and operational environments. Automatic updates on systems should be avoided.

(i) Critical applications should be reviewed and tested whenever there are changes to the operating system, to ensure that no adverse impact on operations or security. A specific group or individual should be given the responsibility to monitor product releases of patches and fixes.

(j) Access to program source code should be restricted to authorised users to prevent the introduction of unauthorised application functionality and to avoid unintentional changes.

(k) Agencies should supervise and monitor outsourced software development.

21.1.9. ICT Security Incident Management

(a) Agencies should ensure ICT security incidents and vulnerabilities associated with ICT systems are communicated in a timely manner for corrective action through the formal reporting procedure for ICT security incident based on:

(i) *Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi*; and

(ii) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam

(b) All personnel, contractors and third party users should be made aware of the procedures for reporting of incidents and vulnerabilities.

(c) All personnel, contractors and third party users are required to note and report any observed or suspected ICT security weaknesses and to report immediately to the ICTSO.

(d) The following incident should be reported immediately to the ICTSO and Agencies CERT/sgCERT/GCERT MAMPU:

(i) Information loss or unauthorised information disclosure

(ii) Suspected information loss or suspected unauthorised disclosure

(iii) Unauthorised or suspected unauthorised usage of ICT system

(iv) Loss or suspected loss, stolen, unauthorised disclosure of access control mechanisms or passwords

(v) Unusual systems behaviour such as missing files, frequent crashes and misrouted messages; and

(vi) Attempted ICT system break-ins and untoward security incidents

(e) Evidence should be collected, retained, and presented to the relevant authorities for follow-up disciplinary and/or legal action.

21.1.10. Business Continuity Management

(a) The objective of Business Continuity Management (BCM) is to ensure continuous functioning of critical business functions and ICT facilities are restored as soon as possible after a disruption.

(b) Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences on ICT security.

(c) Agencies top management should be fully involved in the business continuity risk assessment activities.

(d) Based on the results of the risk assessment, BCM strategy should be developed to determine the overall approach to business continuity.

(e) Agencies top management should approve the BCM strategy created.

(f) The BCM plan to be developed should include at least the following:

(i) A list of core activities which are considered critical with priority rankings;

(ii) A list of personnel both internal and from the vendor together with their contact numbers (facsimile, telephone and e-mail). There should also be a second list to replace personnel who may be unable to attend to the incident;

(iii) A detailed list of information that requires backup and the exact location of storage with instructions on the restoration of information and related facilities;

(iv) Alternative processing resources and locations to replace crippled resources; and

(v) Agreements with service providers for priority resumption of services where possible.

(g) Copies of the BCM plan should be stored in a remote location to escape damage from a disaster at the main site.

(h) The BCM plan should be tested at least once a year or whenever there is a change in the business environment or functions to ensure that it remains effective. Periodic evaluation should be carried out to ascertain that the plan is appropriate and meeting the purpose it was intended for.

(i) Agencies should schedule the testing of the BCM plan to ensure all members of the recovery team and related personnel are aware of the plans, their responsibility and know their roles when the plan is invoked.

(j) Agencies should ensure that copies of the BCM plans are up-to-date and protected as in the main site.

(k) Agencies should determine the owner of the BCM plan.

21.1.11. <u>Compliance</u>

(a) The design, operation, usage and management of ICT systems may be subject to statutory, regulatory and/or contractual requirements. Appropriate procedures should be implemented to ensure compliance to statutory, regulatory and contractual requirements on the use of the system.

(b) Agencies should ensure that all security procedures within their area of responsibility are carried out correctly and regularly reviewed to achieve compliance with security policies and standards. Technical compliance check should be carried out by competent, authorised persons or under the supervision of such persons.

(c) Important records such as pertaining to contracts, licenses, payments and personally identifiable information should be protected from disclosure, loss, destruction and falsification in accordance with business, statutory, regulatory and contractual requirements.

(d) Agencies should develop and implement its data protection and privacy policy and to communicate to all persons involved in the processing of personal information in accordance with the *Personal Data Protection Act 2010*.

(e) Agencies should assure that data are used solely for its intended purpose to protect the privacy of personal information as required under the *Personal Data Protection Act 2010*.

(f) Agencies should ensure that the system for information storage and handling has clear identification of records and retention period and permits appropriate destruction of records after that period if they are not needed by the Agencies as defined by the *State Archives Enactment 1980* and *Sabah State Records and Archives Enactment 2007*.

CHAPTER V: ELECTRONIC RECORDS MANAGEMENT

22. Overview

22.1. Agencies need to keep records of Agencies decisions and transactions to meet the demands of accountability. Records that are created by the day-to-day work in the Government need to be captured, managed and preserved in an organised system which maintains their integrity and authenticity, retaining their value as retrievable organisational records and can be used as primary evidence. Electronic records can exist in many forms and formats such as e-mail, digital image, sound and video, websites, virtual reality models, etc.

22.2. Recordkeeping activities in Agencies are governed by the *State Archives Enactment 1980* and *Sabah State Records and Archives Enactment 2007*, related circulars, guidelines, as well as business and operational needs of the organisation concerned.

23. Objectives

This chapter provides guidelines for minimum requirements pertaining to creation, classification, storage, access, preservation and disposal of electronic records.

24. Scope

24.1. The scope of this chapter covers the following areas:

24.1.1. Acquisition of Electronic Records Management System (ERMS)

24.1.2. Pre-requisites for ERMS implementation

(a) E-file Plan; and

(b) Records Disposal Schedule

24.1.3. Creation of Electronic Records – Metadata Requirement

24.1.4. Maintenance; and

24.1.5. Disposal

(a) Transfer of Records; and

(b) Destruction of Records

25. Acquisition of Electronic Records Management System (ERMS)

Agencies are encouraged to acquire ERMS to create and manage all electronic records. All records management systems must adhere to the mandatory requirements as stated in the "Functional Specifications for ERMS" published by the National Archives of Malaysia.

26. Pre-requisites for ERMS Implementation

26.1. Agencies are required to develop E-file Plan and Records Disposal Schedule as pre-requisite for ERMS implementation. Agencies are encouraged to seek advice from the National Archives of Malaysia via the Sabah State Archives.

26.1.1. <u>E-file Plan</u>

A hierarchical classification tool which, when applied to Agencies information system, can facilitate the capture, titling, retrieval, maintenance and disposal of records.

26.1.2. <u>Records Disposal Schedule</u>

A schedule giving the length of time that records must be maintained and be accessible. At the expiration of the retention period, the records should either be transferred to the Sabah State Archives or be disposed of.

27. Creation of Electronic Records

27.1. Records should be captured electronically into a system that has recordkeeping capabilities to support work processes. Metadata should be assigned and captured together with the records from the time of its creation (refer to the *Standard Metadata Sistem Pengurusan Rekod Elektronik Sektor Awam* prepared by the National Archives of Malaysia).

27.2. In creating and capturing records, Agencies should have in place the following:

27.2.1. A process for identifying appropriate information that should be captured within the working environment;

27.2.2. Workable mechanisms for all record-creating applications to enable the capture of complete elements of a record according to approved formats and standards; and

27.2.3. Links to other records including electronic and paper in other classifications should be established and maintained.

27.3. Metadata Requirement

27.3.1. Metadata is data describing the context, content and structure of records and their management. Metadata allows users to control, manage, find, understand and preserve records.

27.3.2. Some examples of metadata are:

(a) title of a record

(b) subject covered

(c) record format

(d) date of record created

(e) history of record usage; and

(f) details of its disposal

27.3.3. The two (2) main categories of metadata that are used to manage electronic records are recordkeeping metadata and archival metadata. In identifying and capturing appropriate metadata, Agencies should refer to the *Standard Metadata Sistem Pengurusan Rekod Elektronik Sektor Awam* prepared by the National Archives of Malaysia.

28. Maintenance

28.1. To keep electronic records over time, Agencies should consider the following:

28.1.1. appropriate storage devices

28.1.2. facilities for housing them; and

28.1.3. computer systems that generate the records

28.2. Storage conditions should support record protection, easily accessible and cost effective. Stable environmental conditions are necessary to protect digital storage devices which are susceptible to fluctuations in humidity, temperature and radiation.

28.3. Agencies should perform regular and ongoing health and integrity checks of all digital storage devices and their contents to ensure that there is no deterioration and corruption of data.

28.4. Agencies should obtain advice on appropriate storage conditions for computers and information systems and digital storage devices and other aspects of electronic records management from the National Archives of Malaysia via the Sabah State Archives.

28.5. Agencies are required at all times to ensure that:

28.5.1. the record exists – information pertaining to all activities and transactions are recorded;

28.5.2. the record can be accessed – able to locate, access and present information in a way that is true to the original presentation of the information;

28.5.3. the record can be interpreted – can establish when, where and who created it, how it was used and its relation to other information;

28.5.4. the record can be trusted – the information and its representation exactly matches that, which was actually created and used and its integrity and authenticity are demonstrated beyond reasonable doubt;

28.5.5. the record can be maintained – the record can be presented, accessed, interpreted and trusted for as long as necessary, even upon transfer to other approved locations, systems and technologies;

28.5.6. data migration be carried out when there are any technology updates to ensure records can be accessed; and

28.5.7. obsolete databases be given special treatment. Agencies are encouraged to get advice from the National Archives of Malaysia via the Sabah State Archives on how best to preserve those databases.

28.6. Electronic Media Care

Agencies should consider precautionary measures to preserve electronic media over the long-term with a view to ensure continuing accessibility. The precautionary measures are as follows:

28.6.1. Environmental Controls

(a) Store disks and tapes in a vertical position in a dust-free environment.

(b) Store disks and tapes at a constant temperature of 18˚C-20˚C and a constant relative humidity of 35%-45%. Frequent or extreme fluctuations in temperature and humidity can accelerate the deterioration of tape.

28.6.2. Media Controls

(a) Avoid using floppy disks for storage of long-term or permanent records.

(b) Maintain duplicate copies in environmentally controlled storage areas separate from their original location.

(c) Annually test a statistical sample of magnetic tapes and disks to identify any loss of data, to discover and to correct the causes of data loss.

(d) Ensure disk and tape drives are kept clean.

(e) Ensure disks and tapes are kept away from strong electrical or magnetic fields, including telephones.

(f) Ensure unauthorised persons are not allowed access to computers, tapes, disks and documents.

29. Disposal

29.1. Transfer of Electronic Records

Agencies must follow the guidelines and procedures of transferring electronic records specified by the Sabah State Archives.

29.2. Destruction of Electronic Records

29.2.1. Agencies cannot destroy or authorise the destruction of public records which are in their custody or under their control without the prior written approval of the Director, Sabah State Archives.

29.2.2. Agencies should be aware that deletion of records from disk storage is not equivalent to destruction. The document is still retrievable unless a complete secure wiping of the media has taken place. If more than one copy of a record exists, all copies including both primary and working copies should be destroyed at the same time.

29.3. Methods of Destruction

29.3.1. There are several methods of destruction appropriate for the different storage media. Agencies should execute the following:

(a) Magnetic Media

(i) Bulk erase magnetic media by subjecting it to a strong magnetic field; and

(ii) Wipe and reformat magnetic media for secure destruction and for reuse.

(b) Optical Media

(i) Cutting, crushing, or other physical means of destruction of optical media; and

(ii) Wipe and reformat rewritable optical disks for disposal or reuse.

(c) Hard Drives

Wipe and reformat hard drives of personal computers and servers before disposing them.

29.3.2. Agencies should ensure records destruction is:

(a) Appropriate

(i) Irreversible – destruction of records should be irreversible to ensure that the information cannot be recovered by any means; and

(ii) Environmentally friendly – records should be destroyed in an environmentally friendly manner.

(b) Timely

Records should be destroyed within 14 days from the date of obtaining approval from the Sabah State Archives.

(c) Documented

Destruction of all records must be documented.