



# ICT SECURITY REQUIREMENTS FOR ICT BASED FACILITY - GOVERNMENT PERSPECTIVE

Osman Bin Abd.Aziz  
ICT Compliance Division  
MAMPU JPM  
obaa@mampu.gov.my



## BEFORE WE START - GUIDANCE

- EGAA (Electronic Government Activities Act (EGAA 2007))
  - Legal framework for secure electronic government services
  - Enable & facilitate electronic dealings bet Federal Government Agencies with public
- Applies once agency is ready to handle electronic dealings
- Section 9 – Minister issues IT instructions
  - Minimum requirements for agency to undertake electronic transactions
  - Document to Assist / Facilitate / Expedite
  - Not as an impediment
  - Overall idea
    - Protect & Secure ICT Assets
    - Assurance to clients by having the various security processes / measures in place



## IT INSTRUCTIONS - TOC

CHAPTER 1 - INTRODUCTION

CHAPTER 2 - APPLICATION SYSTEM

CHAPTER 3 - ICT SECURITY REQUIREMENTS

CHAPTER 4 - ELECTRONIC RECORDS  
MANAGEMENT



## CHAPTER 3 - SECURITY REQUIREMENTS

### • OVERVIEW

- Our systems are not immune
- Multiple threats multiple sources
- Public service delivery dependent on ICT
- Vigilance against Risks, Threats, Vulnerabilities and Exposures

### INSTRUCTIONS

- Protect information assets against unauthorised access and unauthorised disclosure
- Ensure business continuity
- Agency Head to acknowledge obligation



## SECURITY REQUIREMENTS

# OBJECTIVE

- Protect against loss of Confidentiality, Integrity, Availability, Authenticity and Non-repudiation (CIAANr)
- Achieved through controls
  - policies, processes, procedures, organisational structures, s/w, h/w functions



## SECURITY REQUIREMENTS

### Confidentiality

- To preserve authorized restrictions on information access and disclosure

### INSTRUCTIONS

- Encrypt classified information at storage and transmission using recommended industry standard encryption algorithms that complies with the Digital Signature Act 1997 (Act 562)
- Use Secure Sockets Layer (SSL), Secure Shell (SSH) and Hardware Security Module (HSM) protocols of current versions to secure transmissions end-to-end
- Keep private keys confidential
- All cryptographic keys stored in a secure and tamper proof hardware security module
- Hardware Security Modules (HSMs) support cryptographic algorithms compliant to minimum FIPS 140-2 level 3



## SECURITY REQUIREMENTS

### Integrity

- To safeguard against improper information modification or destruction, errors, omissions, non-repudiation and authenticity

### INSTRUCTIONS

- Incorporate comprehensive built-in checks
- Protect application systems and security infrastructure from external and internal networks attacks



## SECURITY REQUIREMENTS

### Availability

- To ensure on demand access to data and resources to authorised individuals

### INSTRUCTIONS

- Set protection mechanisms to protect against threats that could affect network systems and information availability
- Avoid single point of failure



## SECURITY REQUIREMENTS

### Authenticity

- Assurance that a particular subject (user, program or process) is what he / it claims to be

### INSTRUCTIONS

- Subject prove who it claims to be by providing credentials and authority to perform the requested actions
- All activities are recorded for accountability



## SECURITY REQUIREMENTS

### Non Repudiation

- To provide proof of the integrity and origin of data
- Achieved cryptographically by the use of a digital signature

### INSTRUCTIONS

- Digital signatures comply to the requirements of the Digital Signature Act 1997 (Act 562).



## SECURITY REQUIREMENTS

### Risk Assessment & Treatment Plan

- Agencies to identify RTVE
- Once identified, treatment decisions and appropriate controls must be made to mitigate to an acceptable level

### INSTRUCTIONS

- Apply standard methodology (eg. SPA Bilangan 6/2005 – Garis Panduan Penilaian Keselamatan Risiko Keselamatan Maklumat Sektor awam)
- Perform risk assessment (Security Posture) at least once a year or as and when there are changes in security requirements)



## SECURITY REQUIREMENTS

### SCOPE (11 Domains)

1. Information Security Policy Document
2. ICT Security Management Structure
3. Asset Management
4. Human Resource Security
5. Physical and Environment Security
6. Communications and Operations Management
7. Access Control
8. ICT Systems Acquisition, Development and Maintenance
9. ICT Security Incident Management
10. Business Continuity Management and
11. Compliance Plan



## SECURITY REQUIREMENTS

### 1. Information Security Policy Document

- critical element
- written Information System Security Policy
- define common rules
- overall security direction and guide development

#### INSTRUCTIONS

- Agency shall develop its Information System security policy
- Information security policy shall be relevant, disseminated
- security managed from a single unified administration



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Security server support definition of different security administration rights
- The security server support concept of a group of administrative rights or permitted functions that can be assigned to security managers



## SECURITY REQUIREMENTS

### 2. ICT Security Information Security Management Structure

- Organisational structure to control security

#### INSTRUCTIONS

- A management group in place to ensure support for security initiatives
- A senior officer be appointed as the ICT Security Officer (ICTSO)
- The ICTSO ensure security activities are executed in compliance with Agency Information System Security Policy



## SECURITY REQUIREMENTS

### 3. Asset Management

- Assets are properly managed & protected against unauthorised access & disclosure

#### INSTRUCTIONS

- All information system assets accounted, have an inventory record and a nominated owner
- The inventory information to include type of asset, format, location, backup information, license information and a business value



## SECURITY REQUIREMENTS

### 4. Human Resource Security

- employees can contribute successfully to security
- Equipped with proper training, employees can be depended to identify anomalies and deviations

### INSTRUCTIONS

- Inculcate ICT resources belong to the government
- All users are held responsible for their actions
- All information system support facilities that record and detect user actions
- Users, contractors and third party users be adequately screened



## SECURITY REQUIREMENTS

### 5. Physical & Environment Security

- To prevent unauthorized access, damage and interference
- protection based on the principle of defence-in-depth

### INSTRUCTIONS

- Read together with Arahan Keselamatan
- Critical or sensitive information processing facilities should be housed in secure areas
- Secure areas should be protected allowing only authorized access
- Limit physical access that is necessary for the operation of the information system



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Access points should be controlled and isolated from information processing facilities
- Physical protection against natural or man-made disaster should be designed and applied
- Refer proposals related to buildings, acquisition, lease, renovation, purchase of government and private buildings housing information processing facilities to the Chief Government Security Officer



## SECURITY REQUIREMENTS

### 6. Communications and Operations Management

- Vital to ensure secure and correct operation of information processing facilities
- Develop appropriate operating procedures

### INSTRUCTIONS

- Document and maintain operating procedures and available to all users
- Provide segregation of administration duties and assignment of minimum access rights
- Control changes to information processing facilities and systems
- Separate development, test, and operational facilities



## SECURITY REQUIREMENTS

### BACKUP

- To maintain integrity and availability of information and information processing facilities

### INSTRUCTIONS

- Document backup/restore procedures
- Identify back-up files
- Control access to back-up files to authorised personnel
- Determine frequency of backups
- Store back-up files securely off site
- Test backup files yearly
- Keep 3 generations



## SECURITY REQUIREMENTS

### Audit Trails, Alerts and Reports

- To provide a means of restructuring events, establish accountability and assist in investigations

### INSTRUCTIONS

- Provide audit trails when
  - critical information is accessed
  - network services are accessed
  - special privileges or authorities are used
- Log all events centrally and protect integrity from accidental or intentional changes
- security server to send pre-defined alerts
- Audit logs to capture sufficient details
- Comprehensive standard audit reports of user and security administration activities



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Provide real-time alerts for significant security-related events such as:
  - access attempts that violate the access control rules
  - attempts to access functions or information not authorised
  - concurrent log-on attempts
  - security profile changes
- Audit trails to be kept for a recommended minimum duration of one (1) calendar year



## SECURITY REQUIREMENTS

### 7. Access Control

- Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements

### INSTRUCTIONS

- All access to information system assets shall be defined and documented
  - Need-to-know;
  - Business requirements
  - Minimal access rights
  - Separation of duties
- All access rights and privileges should be reviewed periodically. Privileged access should be restricted and monitored daily by the ICTSO



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Monitor daily access activity to determine unusual activity
- Every user should be identified by a unique identification
- Application security to support the following authentication methods:
  - Normal IDs and passwords; or
  - Certificate-based Public Key Infrastructure (PKI) authentication
- Identification, passwords and authentication information to be kept confidential
- Disable access after 3 failed login attempts
- Set time limit for authentication



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- No automatic right of access will be granted to individuals regardless of their security vetting
- Adopt clear desk clear screen policy



## SECURITY REQUIREMENTS

### 8. ICT Systems Acquisition, Development And Maintenance

- To identify all security requirements at the requirements phase, justified, agreed, and documented prior to development and implementation

### INSTRUCTIONS

- Validate data output from application
- Establish procedure to control installation of software on operational systems
- Implement change through formal change control procedures
- Select, protect and control test data
- Restrict access to program source code to authorised users
- Supervise outsourced software development



## SECURITY REQUIREMENTS

### 9. Information Security Incident Management

- To have a formalised event reporting and escalation procedure
- Refer to 'Pekeliling Am Bil. 1 Tahun 2001 (Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi)
- Awareness to all employees, contractors and third party users

### INSTRUCTIONS

- Report information security events through appropriate management channels quickly
- All employees, contractors and third party users are required to note and report any observed or suspected security weaknesses



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Types of events to be reported to ICTSO
  - Information loss or unauthorised information disclosure or suspected information loss or suspected unauthorised disclosure
  - Unauthorised or suspected unauthorised usage of Information system
  - Loss, stolen or unauthorised disclosure of access control mechanisms or passwords or suspected loss, stolen or unauthorised disclosure of access control mechanisms or passwords
  - Unusual systems behaviour such as missing files, frequent crashes and misrouted messages
  - Attempted Information System break-ins and untoward security incidents
- Establish management responsibilities and procedures to ensure quick, effective, and orderly response to information security incidents
- Collect, retain and present evidence to relevant authorities for disciplinary and or legal action against a person or organization



## SECURITY REQUIREMENTS

### 10. Business Continuity Management

- To ensure continuous functioning of critical business in the event of disruption
- To outline roles and responsibilities
- To ensure information and information processing facilities are restored as soon as possible

### INSTRUCTIONS

- Identify events that can cause interruptions, identify probability, impact and consequence
- Contents of BCM plan to include:
  - A list of core activities with priority rankings
  - A list of personnel available (internal and from the vendor) and replacement
  - A list of information that requires back-up, exact location of storage and instructions on how to restore information and related facilities
  - identification of alternative processing resources and locations
  - agreements with service providers for priority resumption of services where possible



## SECURITY REQUIREMENTS

### INSTRUCTIONS

- Top management be fully involved in BCM activities
- Copies of BCM should be stored in a remote location to escape damage from a disaster at main site
- Test BCM yearly and evaluate effectiveness
- Determine owner of BCM



## SECURITY REQUIREMENTS

### 11. Compliance

- Comply to statutory, regulatory, and contractual security requirements

### INSTRUCTIONS

- Implement procedures on the use of intellectual property rights, copyright, design rights, trademarks, patents, source code licenses and proprietary software products
- Protect important records such as contracts, licences, payments and personally identifiable information from disclosure, loss, destruction, and falsification
- Assure that data captured are used solely for its intended purpose and to accord the privacy of personally identifiable information
- Clear retention period



# REFERENCES

[http://www.mampu.gov.my/mampu/pdf/arahan\\_it\\_bm.pdf](http://www.mampu.gov.my/mampu/pdf/arahan_it_bm.pdf)

<http://www.mampu.gov.my/mampu/pdf/arahanitbi.pdf>



***TTTHANK***

***YOU***

