INFORMATION SECURITY POLICY

ARMED FORCES FUND BOARD (LTAT)

VERSION 3.0
2019

CONTENTS

INTRODUCTION

LTAT's Information Security Policy contains rules that must be read and followed in using Information and Communication Technology (ICT) assets. This policy also makes it clear to all users of their responsibilities and roles in protecting information and assets of LTAT's ICT.

OBJECTIVE

LTAT's Information Security Policy was created to ensure the continuity of LTAT's business by minimizing the impact of ICT security incidents.

The policy also aims to facilitate information sharing in accordance with LTAT's operational needs. This can only be achieved by ensuring all ICT assets are protected.

Meanwhile, the main objectives of LTAT ICT Security are as follows:

a. Ensure smooth operation of LTAT and minimize damage or destruction.

b. Protecting the interests of those who rely on information systems from the effects of failures or weaknesses in terms of confidentiality, integrity, availability, authenticity of information and communication.

c. Prevent misuse or theft of Government ICT assets.

POLICY STATEMENT

Safety is defined as a condition that is free from unacceptable threats and risks. Safety care is an ongoing process. It involves periodic activities that must be done from time to time to ensure security as threats and weaknesses are constantly changing.

ICT information security means the situation in which all arrangements for the provision and provision of ICT-based services run continuously without interruption that may affect security. ICT security is closely linked to the protection of ICT assets. There are four (4) basic ICT security components:

a. Protect LTAT's official secret information and government official information from unauthorized access.

b. Ensuring that every information is accurate and perfect.

c. Ensure availability of information when required by the user.

d. Ensure access to only authorized users or receipt of information from legitimate sources.

LTAT Information Security Policy includes protection against all forms of electronic information is to ensure the security and availability of information to all authorized users. The key features of information security are as follows:

a. Confidentiality -Information may not be disclosed arbitrarily or left unauthorized access.

b. Integrity - Data and information must be accurate, complete and up-to-date. It can only be changed in the allowed manner.

c. Undeniable - The source of data and information should be from legitimate sources and irrefutable.

d. Authenticity - Data and information must be guaranteed authenticity.

e. Availability - Data and information should be accessible at any time.

In addition, steps towards ensuring the safety of information should be based on a rating that is relevant to the current changes to the inherent weaknesses of ICT assets; threats arising from the weaknesses; risks that may arise; and appropriate preventive measures can be taken to address these risks.

SCOPE

LTAT ICT assets consist of hardware, software, services, data or information and people. LTAT's Information Security Policy sets out the following basic requirements:

a. Data and information should be accessed on a continuous basis, quickly, accurately, easily and reliably. This is especially important in order for the results and delivery of services to be done effectively and of quality.

b. All data and information shall be kept confidential and handled as much as possible at all times to ensure the completeness and accuracy of information as well as to protect the interests of the government, services and society.

In order to determine this ICT Asset is guaranteed at all times, this LTAT Information Security Policy covers the protection of all forms of government information that is inserted, created, destroyed, stored, generated, printed, accessed, distributed, in transmitted, and made security copies. This will be done through the creation and enforcement of the control system and procedures in handling all of the following:

a. Hardware

All assets used to support LTAT storage and information processing. Examples of computers, servers, communication tools and so on.

b. Software

Written programs, procedures or regulations and documentation related to computer operating systems stored in the ICT system. Examples of application software or system software such as operating systems, database systems, network system software, or office applications that provide information processing facilities to LTAT;

c. Services

Service or system that supports other assets to perform its functions. Example:

i. Network services such as LAN, WAN, etc.

ii. Office access barrier systems such as the Biodoor system.

iii. Support services such as electrical facilities, air conditioning, fire prevention systems and others.

d. Data or Information

Collection of facts in the form of paper or electronic messages, which contain information to be used to achieve the mission and objectives of LTAT. For example, documentation systems, operating procedures, LTAT records, customer profiles, databases and data files, archive information and more;

e. Man

Individuals who have the knowledge and skills to perform daily job scope LTAT to achieve the mission and objectives of the agency. The individual is an asset based on the tasks and functions performed.

f. Computer And Communications Premises

All facilities and premises used for placing the item **(a) - (e)** above.

Each of the above items needs to be properly protected. Any secret leakage or protection flaw is considered a collision of security measures.

PRINCIPLES

The principles that form the basis of LTAT Information Security Policy and must be complied with are as follows:

a. Access on the basis of need to know

Access to ICT asset utilization is only provided for specific purposes and restricted to specific users on "need to know" only. This means that access will only be granted if the role or function of the user requires that information. Consideration for access is based on the information category as stated in the Safety Instructions document paragraph 53, page 15.

b. Minimum access

User permissions are only given at the minimum set level of reading and / or viewing only. Approval is necessary to enable users to create, store, update, alter or revoke any information. Access rights need to be reviewed from time to time based on the roles and responsibilities of the user / task field.

c. Accountability

All users are held accountable for all their actions on ICT assets. This responsibility should be clearly stated in terms of the sensitivity of an ICT resource. To determine this responsibility is to be followed, the ICT system should be able to support the ease of detecting or verifying that the information system users can be held accountable for their actions.

Accountability or user responsibility includes:

i. Prevents disclosure of information to unauthorized parties.

ii. Checking the information and ensure that it is accurate and complete from time to time.

iii. Specifies information ready to use.

iv. Maintain the confidentiality of the password.

v. Comply with the standards, procedures, measures and established safety guidelines.

vi. Pay attention to classified information especially during the creation, processing, storage, transmission, presentation, exchange and destruction.

vii. Keeping the confidentiality of ICT security measures from being known.

d. Isolation

The task of creating, removing, updating, altering and verifying data must be segregated to avoid unauthorized access and protect ICT assets from errors, leakage of classified information or manipulation.

e. Auditing

An audit is an action for identifying security-related incidents or identifying security threats. It involves the preservation of all records relating to security measures. Thus, ICT assets such as computers, servers, routers, firewalls and network should be determined to generate and keep a log or audit trail of security measures;

f. Compliance

LTAT's Information Security Policy must be read, understood and complied with in order to prevent any form of infringement on it which may pose a threat to ICT security;

g. Recovery

System recovery is essential to ensure availability and accessibility. The main objective is to minimize any disruption or loss resulting from the unavailability. Recovery can be done through duplication activities and establish disaster recovery / service continuity plans; and

h. Interdependency

Each of the above principles is complementary-complementing and relying on one another. Hence, the diversification of approaches in designing and modeling as much as possible safety mechanisms is necessary to ensure maximum security.

ICT SECURITY RISK ASSESSMENT

LTAT should consider the existence of risks on ICT assets as a result of increasing threats and vulnerabilities today. Hence, LTAT should take proactive and appropriate measures to assess the level of risk of ICT assets so that the most effective approaches and results are identified to provide protection and control over ICT assets.

LTAT should implement ICT security risk assessments periodically and continuously depending on technological changes and ICT security requirements. Further follow-up and / or appropriate measures to reduce or control the security risks based on the findings of the risk assessment.

ICT security risk assessment should be carried out on the LTAT information system including applications, software, servers, networks and / or processes and procedures. This risk assessment should also be implemented at premises where information technology resources located including data centers, storage media rooms, utility facilities and other support systems.

LTAT needs to identify appropriate actions to deal with potential risks by choosing the following actions:

a. Reduce risks by implementing appropriate controls.

b. Accept and / or willing to deal with the risks that will occur as long as it meets the criteria set by the Risk Management Committee.

c. Avoiding and / or preventing risks from occurring by taking action that could avoid and / or prevent the occurrence of risk.

d. Transfer the risk to other parties such as suppliers, consultants and other interested parties.

ARTICLE 01 DEVELOPMENT AND MAINTENANCE OF POLICY	
0101 Information Security Policy	
Objective: Describe the direction and management support for information security in accordance with the requirements of LTAT and relevant legislation.	
010101 Policy Implementation	
The implementation of this policy will be carried out by Chief Executive (CE)/ Management Representative (MR) of LTAT as a Chairman of ICT Security Committee (ICTSC) LTAT. The ICTSC consists of Chief Information Officer (CIO), ICT Security Officer (ICTSO) and all Head of Departments.	**CE / Management Representative LTAT**
010102 Spread of Policy	
This policy should be disseminated to all LTAT users (including staff, suppliers, consultants and others)	**ICTSO**
010103 Maintenance of Policy	
LTAT's Information Security Policy is subject to revisions and amendments from time to time including security, procedures and processes control in line with changes in technology, applications, procedures, laws, Government policies and social interests. The following are the procedures in related to the maintenance of the LTAT Information Security Policy: a. Identify and determine the necessary changes. b. Submits the proposed amendments in writing to ICTSO for presentation and approval of the ICT Security Committee Meeting (ICTSC). c. Inform to all users the changes that have been agreed by ICTSC. d. This policy shall be reviewed at least once a year or as it needed by LTAT.	**ICTSO**
010104 Policy Exception	
The LTAT Information Security Policy applies to all ICT LTAT users and no exception.	**All**

ARTICLE 02 SAFETY ORGANIZATION	
0201 Internal Organization Infrastructure	
Objective: Describe the roles and responsibilities of the individuals involved clearly and to achieve the goals of the LTAT Information Security Policy.	
020101 Chief Executive (CE) / Management Representative (MR) LTAT	
The Chief Executive is responsible and in charge of the following: a. Ensure that all users understand the provisions under the LTAT Information Security Policy. b. Ensure that all users comply with the LTAT Information Security Policy. c. Ensure all organizational needs (financial resources, human resources and security protection) are sufficient. d. Ensure risk assessment and ICT security programs are implemented as stipulated in the LTAT Information Security Policy. e. Presiding the LTAT ICT Security Committee Meeting (ICTSC).	**CE / MR LTAT**
020102 Chief Information Officer (CIO)	
Chief Information Officer (CIO) for LTAT is the Assistant General Manager ITMD (Information Technology Management Department). The CIO's roles and responsibilities are: a. Helps CEO in performing tasks involving ICT security. b. Determine ICT security requirements. c. Responsible for matters related to ICT security LTAT.	**CIO**

020103 ICT Security Officer (ICTSO)	
ICT Security Officer (ICTSO) for LTAT is ITMD Manager or Assistant Manager or Senior Executive of Information Technology. The role and responsibilities of the appointed ICTSO are: a. Manage all LTAT ICT security programs. b. Enforce the implementation of the LTAT Information Security Policy. c. Provide information and disclosures concerning the Information Security Policy LTAT to all users. d. Establish guidelines, procedures and procedures in line with the requirements of the LTAT Information Security Policy. e. Conduct risk management. f. Conduct audits, review, formulate a LTAT management response based on findings and provide a report on it. g. Warn against possible harmful threats such as viruses and advise and provide appropriate protection measures. h. Reporting ICT security incident to CIO and LTAT Management. i. Collaborate with all relevant parties in identifying the source of threats or ICT security incidents and recommend prompt remedial measures. j. Provide and implement awareness programs on ICT security. k. Carry out assessments to ensure the level of ICT security and take action on recovery or consolidation to enhance the security of ICT infrastructure to avoid new incidents.	**ICTSO**
020104 Users	
The user has the following roles and responsibilities: a. Read, understand and follow the LTAT ICT Security Policy. b. Knowing and understanding the implications of ICT security impression of its actions. c. Need to go through security screenings if required to deal with official classified information.	**User**

d. Implement the principles of LTAT's Information Security Policy and safeguard the confidentiality of LTAT information. e. Report any activity that threatens ICT and information security to ICTSO immediately. f. Attended awareness programs on ICT and information security. g. Signing of Declaration of Conformity of LTAT Information Security Policy as **Appendix 1**.	
020105 LTAT ICT Security Committee (ICTSC)	
The ICT Security Committee (ICTSC) is responsible for ICT security and serves as an advisor and catalyst in formulating LTAT ICT security plans and strategies. Membership of JKICT LTAT is as follows: Chairman : Chief Executive (CE) Members : 1. Chief Information Officer (CIO) 2. Heads of Departments 3. ICT Security Office (ICTSO) The Secretariat for LTAT ICTSC is the secretariat that conducts the ISMS Review Meeting (ISMS RM). Jurisdiction: a. Approve the LTAT Information Security Policy (ISP) document. b. Monitor the implementation of ICT information security compliance. c. Certify guidelines, procedures and procedures for specific applications in LTAT that comply with the LTAT ISP requirements. d. Analyze suitable technology and propose solutions to ICT security requirements. e. Ensure that LTAT Information Security Policy (ISP) is in line with current government ICT policies. f. Receive reports and discuss current ICT security issues. g. Discuss actions involving violation of LTAT ICT Information Security Policy. h. Decide on the action to be taken on any incident.	**LTAT ICTSC**

020106 LTAT ICT Security Incident Response Team (LCERT)	
Membership of LCERT is as follows: Manager Chief Information Officer (CIO), LTAT. Members 1. ICT Security Officer (ICTSO), LTAT. 2. System Analyst. 3. Senior Information Technology Executive. 4. Information Technology Executive. 5. Computer Programmer. The role and responsibilities of LCERT are as follows: a. Receive and track ICT security complaints and evaluate incidence and type of incident. b. Record and carry out an initial investigation of the incident received. c. Tackle the response of ICT information security incidents and take the minimum remedial action. d. Advise LTAT to take remedial action and strengthening. e. Spread information related to strengthening ICT information security to LTAT.	

0202 Third Party	
Objective: Ensure the safety of all ICT assets used by third parties (Suppliers, Consultants and others).	

020201 Requirement of Security Contract with Third Party	
This is to control the process and use of information by third party. Things to keep in mind include the following: a. Read, understand and comply with LTAT's Information Security Policy.	**CIO, ICTSO, ICT Manager, System Admin and Third**

	Party
b. Identify information security risks, information processing facilities and implement appropriate controls before authorizing the access. c. Identify security requirements before granting access or use permission to third parties. d. Access to LTAT ICT assets must be based on contractual agreements. e. Ensure that all safety conditions are clearly stated in agreement with a third party. The following shall be included in the agreement entered into. i. LTAT Information Security Policy. ii. Security Screening. iii. Certificate of Official Secrets Act 1972. iv. Intellectual property right.	

ARTICLE 03 ASSET MANAGEMENT	
0301 Asset Accountability	
Objective: Provide and support appropriate protection against all LTAT ICT assets	
030101 ICT Assets Inventory	
This is to ensure that all ICT assets are given proper control and protection by their respective owners or trustees. Things to keep in mind include the following: a. Ensure that all ICT assets are identified and asset information is recorded in the capital and inventory register forms and is constantly updated. b. Ensure that all ICT assets are owned and operated by authorized users only. c. Ensure that all users confirm the placement of ICT assets placed in LTAT. d. The rules for the handling of ICT assets must be identified, documented and implemented. e. Each user is responsible for all ICT assets under his / her control.	**System Admin & All**
0302 Classification and Control of Information	
Objective: Ensure that every ICT information or asset is provided with appropriate level of protection.	
030201 Classification of Information	
Information must be classified or labelled accordingly by the authorized officer in accordance with the Security Instructions document. Every classified information must have the security level as it set out in the Security Instructions document as follows: a. Big Secret. b. Secret. c. Confidential. d. Limited.	**All**

030202 Information Handling	
Information handling activities such as collecting, processing, storing, transmitting, conveying, changing and destroying shall take the following security measures: a. Prevents disclosure of information to unauthorized parties. b. Checking the information and determine it is accurate and complete from time to time. c. Specifies information ready for use. d. Maintain the confidentiality of the password. e. Comply with established standards, procedures, measures and safety guidelines. f. Pay attention to classified information especially during the creation, processing, storage, transmission, delivery, exchange and destruction. g. Keeping the confidentiality of ICT security measures from being publicly known.	**All**

ARTICLE 04
HUMAN RESOURCES SAFETY

0401 Human Resource Safety in Daily Tasks

Objective:

Ensure all human resources involved include LTAT officers and staff, suppliers, consultants and stakeholders to understand their responsibilities and roles as well as to enhance their knowledge of ICT asset security. All LTAT staff must comply with the current terms and conditions of service and regulations in force.

040101 Before Service

Things that must be followed including: a. Fully and clearly state the roles and responsibilities of LTAT officers and staff and third parties involved in securing ICT asset security before, during and after service. b. Conduct security screening for LTAT officers and employees and third parties involved based on applicable legal, regulatory and ethical requirements that are in line with service requirements, level of information to be achieved and expected risks. c. Adhere to all terms and conditions of service offered and current regulations based on the agreement set.	**All**

040102 In Service

Things that must be followed including: a. Ensure LTAT officers and staff and stakeholders manage the security of ICT assets based on the laws and regulations set by LTAT. b. Ensure awareness training and related safety management of ICT assets are given to LTAT ICT users on an ongoing basis in discharging their duties and responsibilities, and if necessary, to be given to interested third parties from time to time. c. Ensure that there is a disciplinary process and / or legal action on LTAT officers and staff and interested third parties in the event of a breach with the legislation and regulations specified by LTAT. d. Strengthen knowledge related to the use of ICT assets to ensure every ICT facility is utilized in the proper way to ensure the importance of ICT security. Any required training and technical training, the user may refer to the Finance & Administration Department (FAD).	**All**

040103 Exchange or End of Service	
Things to keep in mind include the following: a. Ensure that all ICT assets are returned to LTAT according to the rules and / or specified terms of service. b. Revoke or withdraw all access permissions on the information and facilities of the information process in accordance with the rules and / or term of service set by LTAT.	**All**

ARTICLE 05
PHYSICAL AND ENVIRONMENT SECURITY

0501 Area Security

Objective:

Protect premises and information from any form of intrusion, threats, damages and unauthorized access.

050101 Area Control

This is to prevent physical access, damage and disturbance to the premises and agency information.

Things to keep in mind include the following:

a. Physical security areas should be clearly identified. The location and strength of physical safety should depend on the need to safeguard assets and risk assessment results.

b. Using perimeter security (wall barriers, control fences, security guards) to protect areas containing information and information processing facilities.

c. Installing an alarm device or security camera.

d. Restrict the entrance and exit.

e. Establish control counters.

f. Provide a special place or room for visitors.

g. Establish security control services.

h. Protecting limited areas through proper entrance controls to ensure only authorized staff can access this gateway.

i. Design and implement physical security in offices, rooms and facilities.

j. Design and implement physical protection from fire, flood, explosion, chaos and disaster.

k. Provide guidelines for staff working in limited areas.

l. Ensure delivery and shipment areas and other places are controlled from unauthorized parties.

All

050102 Physical Entrance Control	
The matters to be observed include the following: a. Entrance controls for each floor in the LTAT Building are controlled by the Biodoor system (finger or employee's smart card) and CCTV system.	**All**
050103 Prohibited Area	
The prohibited area is defined as a restricted area of entry to certain officers only. This was done to protect the ICT assets that exist within the area. LTAT's prohibited areas are file rooms, server rooms, rack switches and PABX rooms. a. Access to restricted areas is only for authorized officers. b. Third parties are strictly forbidden to enter restricted areas except for certain cases such as providing technical support or support services, and they must be accompanied at all times until the duty at the area is completed.	**FAD**
0502 Safety of Equipment	
Objective: Protect LTAT ICT equipment from loss, damage, theft and disruption of the equipment.	
050201 ICT Equipment	
The matters to be observed are as follows: a. Users should check and ensure that all ICT equipment under their control is functioning properly. b. Users are solely responsible for their respective computers and are not allowed to change any hardware and configuration. c. Users are strictly forbidden to add, remove or replace any established ICT hardware. d. Users are prohibited from installing any additional software without the permission of the ICT System Administrator. e. User is responsible for the damage or loss of ICT equipment under their control. f. Users must ensure their antivirus software on their personal computers is always active and updated while scanning on any storage media.	**All**

g. The use of passwords for access to computer systems is compulsory.

h. All ICT support equipment shall be protected against theft, damage, misuse or unauthorized modification.

i. Critical equipment should be supported by Uninterruptable Power Supply (UPS).

j. All ICT equipment should be stored or placed in an orderly, clean place and has safety features. Network equipment such as switches, hubs, routers and others should be placed in special shelves.

k. All equipment used continuously must be placed in an air-conditioned and ventilated area.

l. Any ICT equipment to be taken out of LTAT premises, it must be approved by FAD and recorded for monitoring purposes.

m. Missing ICT equipment should be reported to FAD immediately.

n. Handling of ICT equipment shall comply with and refer to current regulations in force.

o. Users are not allowed to change the computer's position from where it was placed without FAD's permission.

p. Any damage to ICT equipment shall be referred to the Incident Management procedure for repairing.

q. Any stickers other than for official purposes are not allowed. This is to ensure the equipment is always in good condition.

r. IP address configuration is not allowed to be changed from the original IP address.

s. Users are strictly prohibited from changing passwords for administrators (administrator passwords) that have been set by the ICT System Administrator.

t. Users are responsible for the hardware, software and information under their care and should be used solely for official business.

u. Users must ensure that all computer hardware, printers and scanners are "OFF" when leaving the office.

v. Any form of misappropriation or misuse of ICT equipment shall be reported to ICTSO.

050202 Storage Media	
Storage media is an electronic equipment used to store data and information such as compact discs, USB drives, CDROMs, thumb drives and other storage media. Storage media must be in good condition, safe, secure confidentiality, integrity and availability for use. The matters to be observed are as follows: a. The storage media should be kept in good storage space and have security features appropriate to the content of the information. b. Access to storage media storage areas should be restricted to authorized users only. c. All storage media should be controlled to prevent unauthorized access, theft and destruction. d. Access and storage of storage media should be recorded. e. The backup hardware must be placed in a controlled place. f. Make a copy or backup on second storage media for security purposes and to avoid data loss. g. All data storage media to be disposed of must be deleted in a safe and secure manner. h. Deleting information or media content must first obtain the owner's informed consent.	**All**
050203 Software and Applications Media	
Things to keep in mind are as follows: a. Only certified software is allowed for LTAT use. b. Internal application systems are not allowed to be demonstrated or distributed to other parties except with the permission of the Head of Department. c. Source code of a system should be kept in order and any amendment must be in accordance with the prescribed procedure.	
050204 Hardware Maintenance	
Hardware should be maintained properly to ensure availability, confidentiality and integrity. The matters to be observed are as follows:	**FAD**

a. All the equipment maintained shall comply with the specification set by the manufacturer. b. Ensure that the hardware can only be maintained by staff or authorized parties only. c. Responsible for every hardware maintenance either within the warranty period or has expired warranty period. d. Check and test all hardware before and after the maintenance process. e. Inform users before performing maintenance on schedule or on purpose. f. All maintenance must be approved by FAD.	
050205 Equipment Outside of Premises	
Hardware brought out of the LTAT premises is vulnerable to various risks. Things to keep in mind are as follows: a. Equipment should be protected and controlled at all times. b. Storage or placement of equipment must have appropriate safety features.	**All**
050206 Hardware Disposal	
Disposal involves all damaged, obsolete and non-repairable ICT equipment whether the capital property or inventory supplied by LTAT and placed in LTAT. The ICT equipment to be disposed of should be through the current disposal procedures. Disposal should be done in a controlled and complete manner so that information cannot be missed from LTAT control. The matters to be observed are as follows: a. All contents of the equipment, especially the official secret information, shall be deleted first before disposal either through shredding, grinding, degaussing or burning. b. If the information needs to be stored, then the user may create duplication.	**All, JKP Officers dan ITM Officers**

c. The ICT equipment to be disposed of prior to transfer must be ensured that the data in the storage has been removed in a safe manner.

d. DAF officers should identify whether certain equipment can be disposed of or not.

e. The equipment to be disposed of shall be stored in a designated area with safety features to ensure the safety of the equipment.

f. The FAD officer is responsible for recording the details of the disposal and updating the records of the disposal of ICT equipment into the SPA inventory system.

g. Disposal of ICT equipment should be centred and according to current disposal procedures.

h. ICT users are **NOT ALLOWED** from doing the following things:

i. Store any ICT equipment to be disposed of for personal use. Unplug, remove and store additional hardware in CPU like RAM, hard drive, motherboard, etc.

ii. Store and transfer external computer hardware such as AVR, speakers and any related equipment to any part of LTAT.

iii. Moving out of LTAT any ICT equipment to be disposed.

iv. Dispose ICT equipment by their self. Disposal is only can be done under LTAT's responsibility.

v. The user is responsible for ensuring that all confidential information in the computer is copied to the second storage media such as diskette or thumb drive before removing such information from the device to be disposed.

0503 Environmental Safety

Objective:

Protecting LTAT ICT assets from any form of environmental threats caused by natural disasters, errors, negligence or accidents.

050301 Environmental Control	
To avoid damage and disruption of premises and ICT assets. To ensure the safety of the environment, the following points should be observed: a. Plan and prepare the entire data layout of the data center (printing room, computer equipment and office space etc.) properly. b. All office space in particular areas with ICT facilities shall be equipped with adequate security protection such as fire prevention and emergency exit. c. Protective equipment should be placed in appropriate location, easily recognizable and operated. d. Flammable materials should be stored outside the ICT asset storage area. e. All liquids must be placed in a appropriate location and far from ICT assets. f. Users are prohibited from smoking or using cooking appliances such as electric kettles near computer equipment. g. All protective equipment should be checked and tested at least two (2) times a year. The activities and results of these tests should be recorded to facilitate for references and actions where necessary; and Access to the riser channel should always be locked.	**All**
050302 Power supply	
Power supply is the source of electricity supplied to ICT equipment. The matters to be observed are as follows: a. All ICT equipment should be protected from power failures and electricity supplies should be channeled to the appropriate ICT equipment. b. Supporting equipment such as Uninterruptable Power Supply (UPS) and generator can be used for critical services such as in server rooms to obtain continuous power supply. c. All power supply support equipment should be reviewed and tested on a scheduled basis.	**FAD & PPHM**

050303 Cable	
Computer cables should be protected as they may cause information to become vulnerable. The security measures to be taken are as follows: a. Use cables that follow specifications. b. Protects wires from accidental or unintentional damage. c. Protect the cable installation route completely to avoid the threat of damage and wiretapping. d. All cables should be clearly labelled and must go through the cable trunking to ensure security from damage and intercept information.	**ITMD & PPHM**
050304 Emergency Procedures	
Things to keep in mind are as follows: a. Each user should read, understand and adhere to emergency procedures. b. Environmental emergencies such as fires should be reported to LTAT Incident Officer.	**FAD**
0504 Document Security	
Objective: Protect LTAT information from any form of environmental threats caused by natural disasters, errors or negligence.	
050401 Document	
The matters to be observed are as follows: a. Each document must be filed and labeled according to security classifications such as Open, Limited, Confidential, Secret or Big Secrets. b. The movement of files and documents should be recorded and should follow the safety procedures. c. Loss and damage to all types of documents should be notified in according to the Safety Instructions procedure. d. Document disposal should follow current security procedures such as Safety Directives, Practice Instructions (Record Disposal Closes) and the procedure of the National Archives Department. e. Use encryption at official confidential documents and transmitted electronically.	**All**

ARTICLE 06
OPERATION AND COMMUNICATION MANAGEMENT

0601 Operating Procedures Management

Objective:
Ensuring the management of the operation works properly and securely from any threats and disruptions.

060101 Procedure Control

The matters to be observed are as follows: a. All operational management procedures established, identified and applied shall be documented, stored and controlled. b. Each procedure must contain clear, organized and complete instructions such as capacity requirements, handling and processing of information, handling and transmission of errors, output handling, technical assistance and recovery if processing is interrupted or stopped. c. All procedures should be updated from time to time or as needed.	**All**

060102 Change Control

Things to keep in mind are as follows: a. Modifications involving hardware, systems for information processing, software, and procedures must be authorized by top management or owners of ICT assets. b. Activities such as installing, maintaining, removing and updating any component of the ICT system shall be operated by the authorized party or officer and have knowledge or is directly involved with the relevant ICT assets. c. All modifications to the components of the ICT system must comply with the specification that have been set. d. All change or modification activities shall be recorded and controlled to prevent any error whether intentionally or not.	**All**

060103 Segregation of Duties and Responsibilities

The matters to be observed are as follows: a. The scope of duties and responsibilities should be segregated to minimize the possibility of abuse or unauthorized modification of ICT assets.	**All**

b. The tasks to create, remove, update, alter and verify data should be segregated to prevent unauthorized access as well as protect ICT assets from errors, leakage of classified information or manipulation. c. Hardware used for developing, updating, maintaining and testing applications should be isolated from hardware used to production. Isolation also includes the separation between operations and network groups.	
0602 Management of Third-Party Service Delivery	
Objective: Ensure the implementation and maintenance of appropriate information security and service delivery levels in line with service agreements with third parties.	
060201 Delivery Service	
The matters to be observed are as follows: a. Ensure security control, service definition and level of service contained in the agreement are complied, implemented and maintained by third parties. b. Services, reports and records submitted by third parties should be regularly monitored and reviewed from time to time. c. Management of policy changes need to be based on the critical level of systems and processes involved and risk review.	**All**
0603 System Planning and Acceptance	
Objective: Minimize the risks that cause disruption or system failure.	
060301 Capacity Planning	
The capacity of a component or ICT system should be carefully planned, managed and controlled by relevant officers to ensure that its requirements are adequate and appropriate for the development and use of the ICT system in the future. These capacity requirements also need to comply with ICT security features to minimize risks such as service disruptions and losses due to unplanned modifications.	**ITMD**

060302 System Acceptance	
All new systems (including updated or modified systems) shall meet the prescribed criteria prior to acceptance or approval.	**ITMD**
0604 Malicious software	
Objective: Protect software integrity and information from disclosure or damage caused by malicious software such as viruses, trojans, and so on.	
060401 Protection from Malicious Software	
Things to follow in protecting from malicious software are as follows: a. Install security systems for detecting malicious software or programs such as anti-virus, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) and according to proper and secure usage procedures. b. Install and use only genuine, registered and protected software under any applicable written law. c. Scan all software or systems with anti-virus before using them. d. Updates anti-virus with the latest antivirus pattern. e. Periodically check system or information content to detect undesirable activities such as loss and damage to information. f. Attends awareness raising on malicious software threats and how to handle them. g. Liability clause in the contract that was offered to the software provider. This clause is intended for recovering claims if the software contains malicious programs. h. Conduct quality assurance programs and procedures on all developed software. i. Warned about ICT security threats such as virus attacks.	**All**
060402 Protection from Mobile Code	
The use of mobile code that can jeopardize ICT security is not permitted.	**All**

0605 Housekeeping

Objective:
Protect the integrity of the information to be accessible at any time.

060501 Backup

To ensure that the system can be rebuilt after a disaster. Backup should be performed every time the configuration changes.

Things to keep in mind are as follows:

a. Make security backups on all software systems and applications at least once or after getting the latest version.

b. Backup all data and information according to operating requirements. Backup frequency depends on the critical level of information.

c. Testing backup systems and existing recovery procedures to ensure they work perfectly, reliably and effectively when used especially during emergencies.

d. Records and stores backup copies in different locations and secured.

All

0606 Network Management

Objective:
Protect information in network and support infrastructure.

060601 Network Infrastructure Control

Network infrastructure must be controlled and managed as best as possible to protect threats to systems and applications within the network.

The matters to be observed are as follows:

a. Network equipment should be placed in a location that has a strong and risk-free physical property such as flood, vibration and dust.

b. Access to network equipment should be controlled and restricted to authorized users only.

c. Firewalls should be installed and configured and supervised by ITMD.

d. All incoming and outgoing traffic must pass through a firewall under ITMD control.

ITMD

e. All sniffer or network analyzer software is prohibited to be installed on the user's computer unless it obtains ICTSO permission. f. Install the Intrusion Prevention System (IPS) software to detect any intrusion attempts and other activities that could threaten the LTAT system and information. g. Install Web Content Filtering on the Internet Gateway to block prohibited activity. h. Any network connection that is not under the control of LTAT is not allowed. i. All users are only allowed to use the LTAT network only and the use of Modem / USB Broadband is strictly prohibited. j. The facilities of wireless LANs should have security control.	
0607 Media Management	
Objective: Protecting ICT assets from any disclosure, modification, transfer or destruction and interruption of service activities.	
060701 Media Transmission and Transfer	
Transmission or transfer of media out of office must first obtain permission from the owner.	**All**
060702 Media Control Procedures	
Media control procedures that need to be followed are as follows: a. Labeling all media according to the level of sensitivity of an information. b. Limit and specify media access to authorized users only. c. Restrict data or media distribution for authorized purposes only. d. Controls and records media maintenance activities to avoid any unauthorized damage and disclosure. e. Keep all the media in a safe place. f. Media that contains classified information to be removed or destroyed must be disposed accordingly with proper and secure procedures.	**All**

060703 Documentation Security System	
The items to be followed in ensuring the safety of the documentation system are as follows: a. Ensure the documentation storage system has security features. b. Provide and enhance the security of the documentation system. c. Controls and records all existing documentation access activities.	**All**
0608 Information Exchange Management	
Objective: Ensuring the security of information and software exchange between LTAT and external agencies is assured.	
060801 Information Exchange	
Things to keep in mind are as follows: a. A formal information exchange policy, procedure and control should be established to safeguard the exchange of information through the use of various types of communication facilities. b. Agreements (Acts & Regulations) need to be established for the exchange of information and software between LTAT and external agencies. c. Media that contains information needs to be protected against unauthorized access, misuse or damage during exit transfer from LTAT. d. Information contained in electronic mail should be protected.	**All**
060802 Electronic Mail Management (Email)	
The use of email at LTAT should be monitored continuously by the Email Administrator to meet the e-mail and Internet usage ethics requirements contained in *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003* entitled *"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* and any written law in force. The matters to be followed in handling electronic mail are as follows: a. Accounts or email addresses (e-mails) provided by LTAT can only be used. Use of the accounts belonging to someone else or a shared account is prohibited. b. Official email delivery must use an email account official and make sure the recipient's email address is correct.	**All**

c. Users are advised to use a file, if necessary, not exceeding twenty megabytes (20Mb) during transmission. Compression methods to reduce size are recommended. d. Users should avoid opening emails from unknown or unknown senders. e. The user must identify and verify the identity of the user who is communicating with him before proceeding to the transaction of information via e-mail. f. Every official e-mail sent or received must be kept according to the designated electronic file management system. g. Emails that are not important and have no archived values that have been taken and are no longer needed can be deleted. h. The user should determine the date and time of the computer system is accurate. i. Take action and respond quickly to email and take immediate action. j. Users should be responsible for updating and using their respective mailboxes.	
060803 General information	
Things to keep in mind in ensuring information security are as follows: a. Ensure software, data and information are protected by appropriate mechanisms. b. Ensure system accessible to the public is first tested. c. Ensure that all information to be displayed is approved and approved before uploading to the website.	**All**
0609 Monitoring	
Objective: Ensure detection of unauthorized information processing activities.	

060901 Audit Trail	
Each system must have an audit trail. The audit trail records the activities that occur in the system chronologically to permit inspection and reconstruction done for the arrangements and changes in an event. An audit trail shall contain the following information: a. Record every transaction activity. b. Audit trail information contains the user identity, source used, change of information, date and time of activity, network and application used. c. The user's access activity on the ICT system is either legitimate or not.	**ICT System Admin**
060902 Log System	
The Administrator of the ICT System shall perform the following: a. Create a log system to record all daily activity of users. b. Checks the log system periodically to detect errors that cause system interruptions and take corrective action immediately. c. Should there be other illegal activities such as information theft and intrusion, the ICT System Administrator should report to ICTSO and CIO.	**System Owner**
060903 Log Monitoring	
Things to keep in mind are as follows: a. Audit logs that record all activities need to be generated and are kept for an agreed period of time to assist in the investigation and monitoring of access control. b. Procedures for monitoring the use of information processing facilities should be established and the results should be monitored periodically. c. All records and log information need to be protected from modified and any unauthorized access. d. The time associated with the information processing system in LTAT or the security domain needs to be aligned with an agreed-upon time source.	**System Owner**

ARTICLE 07
ACCESS CONTROL

0701 Access Control Policy

Objective:
Controlling access to information.

070101 Access Control Requirements

Access to processes and information should be controlled according to different user function and safety requirements. It needs to be recorded, updated and supported by existing user access control policy. Access control rules should be established, documented and reviewed based on service and security requirements. The matters to be observed are as follows: a. Controls access to ICT assets in according to security requirements and user roles. b. Controlling access to internal and external network services. c. Controlling information security is achieved using mobile facilities or equipment. d. Controlling access to information processing facilities.	**LTAT & ICTSO**

0702 User Access Management

Objective:
Controls user access to LTAT ICT assets.

070201 User's account

Each user is responsible for the ICT system they use. In order to identify the users and activities performed, the following points should be observed: a. Only accounts designated by LTAT can be used. b. User accounts must be unique and should reflect user identity. c. User account ownership is not an absolute right of a person and it is subject to LTAT rules. The account may be withdrawn if the use violates the rules.	**FAD**

d. Use of the accounts belonging to someone else or a shared account is prohibited. e. The ICT System administrator may freeze and terminate the user's account for the following reasons: i. Changing the scope of work. ii. Retired. iii. Service terminated.	
070202 Access Rights	
Determining and applying access rights should be given strict control and supervision based on the requirements of the job scope.	**FAD**
070203 Password Management	
The selection, use and management of passwords as the main gateway for information and data in the system must comply with the best practices and procedures set by LTAT as follows: a. Under no circumstances and reasons, passwords must be protected and should not be shared with anyone. b. Users have to change the password when suspected of leakage or compromised password. c. Password length must be at least eight (8) characters with a combination of number and symbol characters. d. Passwords should be remembered and CAN NOT be recorded, stored or disclosed in any way. e. Password windows and screen saver should be activated especially on computers that are located in areas of common space. f. Passwords should not be displayed during input, in reports or other media and cannot be encoded within the program. g. Enforce password change during login first time or after login the first time or after the password is reset. h. Passwords should be different from the identification of the user identity (ID). i. Password must be changed after 90 days or after appropriate	**All & ICT System Admin**

time. j. Avoid reuse of recently used password. Note: The use of the password for the above criteria is not subject to use of the password on the IBM i-Series server	
070204 Clear Desk and Clear Screen	
All information in any form of media must be kept in good order and safe to avoid damage, theft or loss. Clear Desk and Clear Screen means not leaving sensitive materials are exposed either on the table or on the display screen when the user is not in place. Things to keep in mind are as follows: a. Use password screen saver or logout when leaving the computer. b. Store sensitive materials in a drawer or locked file cabinet. c. Make sure all documents are taken immediately from printers, scanners, fax machines and photocopiers.	**All**
0703 Network Access Control	
Objective: Prevents unauthorized access to network services.	
070301 Network Access	
Access control of network services should be secured by: a. Placing or installing an appropriate interface between LTAT networks, other agency networks and public networks. b. Establish and enforce a mechanism for authentication of users and devices that meet suitability for use. c. Monitor and enforce user access control over ICT network services.	**ITMD**
070302 Internet access	
The matters to be observed are as follows: a. Use of the Internet at LTAT should be monitored continuously by ITMD to ensure its use for authorized access purposes only. Vigilance will be able to protect against the ingress of malicious code, viruses and materials that are not supposed to in a series of LTAT. b. Content Filtering method must be used to control Internet access according to work function and monitoring of compliance level.	**ITMD Manager & All**

c. Use of packet shaper technology to control activity (video conferencing, streaming video, chat, downloading) is necessary to manage the maximum and more effective use of bandwidth (bandwidth).

d. Internet use is for official use only. ICT Managers have the right to determine which users are allowed to use the Internet or otherwise.

e. The sites visited should only be related to the field of work and are limited for purposes permitted by Management / authorized officers.

f. The material obtained from the Internet should be determined by its accuracy and validity. As a best practice, Internet resource references should be stated.

g. Official materials should be reviewed and verified by the Head of Department before being uploaded to the Internet.

h. Users are only allowed to download legitimate materials such as software registered and is under copyrighted.

i. Any material downloaded from the Internet should be used for purposes authorized by LTAT.

j. Only authorized officers can use public discussion facilities such as newsgroups and bulletin boards. However, the content of this public discussion should be approved by Management first in accordance with the established policies and regulations.

k. Users are prohibited from doing the following activities:

   i. Upload, download, store and use unlicensed software and any applications such as electronic games, videos, songs that may affect the level of internet access.

   ii. Prepare, upload, download and save material, text of speech or materials containing obscene elements.

0704 Operating System Access Control

Objective:
Prevents unauthorized access to the operating system

070401 Operating System Access	
Operating system access control is necessary to prevent any unauthorized access. Security facilities in the operating system should be used to prevent access to computer system resources. This facility is also necessary for: a. Identify identities, terminals or locations for each authorized user. b. Record of successful and failed access. The methods used must be capable of supporting the following: a. Validating authorized users. b. Creating an audit trail on all operating system achievements, especially users with level super user. c. Generate alerts in the event of a breach of system safety rules. Things to keep in mind are as follows: a. Control access to the operating system using secure log on procedures. b. Create a unique identifier (ID) for each user and only for those users. c. Limit and control the use of the program. d. Limit the connection to a high-risk app.	**ITMD**
0705 Application and Information Access Control	
Objective: Prevents unauthorized access to information contained in the application system.	
070501 Application and Information Access	
It aims to protect the existing system of application and information from any unauthorized access that may cause damage. the following must be followed to ensure system and application access controls are solid: a. Users may only use information systems and applications that are permitted according to the level of access and security of the specified information. b. Every access for information system and user application should	**System Admin**

be recorded (log system). c. Limit certain system and application access to three (3) attempts. Failure will result in the user's account or password being blocked. d. Ensure network system controls are robust and complete with security features to prevent unauthorized activity or access. e. Access to information systems and applications is remotely limited to only authorized service and staff.	
0706 Mobile Equipment and Remote Work	
Objective: Ensure the safety of information while using mobile devices and remote work facilities.	
070601 Mobile Devices	
Things to adhere to are as follows: a. Mobile equipment should be stored and locked in a safe place when not in use. b. Officers and staff who use mobile equipment is responsible for ensuring the security of information and equipment.	**All**
070602 Remote Work / Long Distance Work	
Things to be observed are as follows: a. Protection measures should be taken to prevent loss of equipment, disclosure of information and illegal access and abuse of facilities.	**All**

ARTICLE 08 PROCUREMENT, DEVELOPMENT AND MAINTENANCE SYSTEM	
0801 Security in Developing Systems and Applications	
Objective: To ensure that the system developed in-house or third party have an appropriate ICT security.	
080101 Information System Safety Requirements	
The matters to be observed are as follows: a. System acquisition, development, enhancement and maintenance must have security controls to ensure that no error can interfere with the processing and accuracy of information. b. Security tests should be performed on the input system to check the validity and integrity of the entered data, the processing system to determine whether the program works properly and perfectly. c. Applications must contain validation checks to prevent any information damage due to processing errors or intentional treatment. d. All systems developed either internally or externally should be tested in advance to ensure that the system meets the safety requirements set before use.	**System Owner**
080102 Input and Output Data Validation	
Things to keep in mind include the following: a. Input data for the application needs to be verified to ensure that the data entered is correct and appropriate. b. Output data from applications need to be verified to ensure that the resulting information is accurate.	**System Owner**
0802 System File Security	
Objective: Ensure that the system files are controlled and operated properly and safely.	
080201 System File Control	
Things to keep in mind are as follows: a. System file updating process may only be performed by the ICT System Administrator or responsible officer and accordingly with the prescribed procedure.	**System Owner & ICT System Admin**

b. The updated system code or program can only be implemented or used after testing. c. Controls access to program codes or programs to prevent damage, unauthorized modification, deletion and theft. d. Test data should be carefully selected, protected and controlled. e. Enable log audit to record all updating activities for statistical, recovery and security purposes.	
0803 Security in Development and Support Process	
Objective: Maintain and secure information system and application security.	
080301 Change Control Procedures	
Things to keep in mind are as follows: a. Changes or modifications to information systems and applications shall be controlled, tested, recorded and verified prior to application. b. Critical applications need to be reviewed and tested when there is a change to the operating system to ensure there is no adverse effect on agency operations and security. Individuals or a particular group should be responsible for monitoring the improvements and corrections made by the vendor. c. Controlling changes and / or amendments to software packages and make sure any changes are limited to the requirements only. d. Access to the source code of the application must be restricted to authorized users. e. Prevents any opportunity to leak information.	**System Owner & ICT System Admin**
080302 Software Development Outsourced	
a. Outsource software development needs to be managed and monitored by system owners.	**Section IT & ICT System Admin**

0804 Vulnerability Technical Control	
Objective: Ensuring technical control of vulnerability is effective, systematic and periodic by taking appropriate measures to ensure its effectiveness.	
080401 Control of Technical Threats	
These technical controls need to be implemented on all operating systems and application systems. Things to adhere to are as follows: a. Obtain timely vulnerability technical information on the timing of the information system used. b. Assessing the level of vulnerability to identify the level of risk that may be encountered. c. Take control measures to address related risks.	**ICT System Admin**
0805 Cryptography Control	
Objective: Protect the confidentiality, integrity and legitimacy of information through cryptographic controls.	
080501 Encryption	
Users must make encryption of sensitive information or official secret information at all times.	**All**
080502 Digital Signature	
The use of digital signatures is required by all users, specifically those who manage electronic secret information transactions electronically.	**All**
080503 Public Key Infrastructure Management (PKI)	
Management of the PKI shall be affected and safely to protect the keys from being altered, destroyed and compromised over the validity of key. Any changes should be recorded for security purposes and the duration of the validity period of the key.	**All**

ARTICLE 09
SECURITY INCIDENT MANAGEMENT CONTROL

0901 ICT Security Incident Reporting Mechanism

Objective:
Ensure incidents are handled quickly and effectively to minimize the impact of ICT security incidents.

090101 Reporting Mechanism

ICT security incidents mean the adverse event that occurs on ICT assets or threats of possible occurrences. It may be an act that violates the Information Security Policy whether express or implied. The following ICT security incidents should be reported to ICTSO and Management immediately: a. The information obtained is lost, disclosed to unauthorized parties or, suspected of being lost or disclosed to unauthorized parties. b. Information systems are used without such permission or suspicion. c. Passwords or access control mechanisms are lost, stolen or disclosed, or suspected to be lost, stolen or disclosed. d. Occurring incredible system incidents like losing files, frequent system failures and sending error messages. e. Experiment attempts, intruders and incident incidents are unexpected. Summary of all work processes involved in the reporting of ICT security incidents in LTAT as the SP-LTAT-20000 ICT-Incident Management (Incident Management).	**All**

0902 ICT Security Incident Management Information

Objective:
Ensure consistent and effective approaches are used in ICT security incident management information.

ARTICLE 10
SERVICE CONTINUITY MANAGEMENT

1001 Service Continuity Policy

Objective:
Ensure service operations are uninterrupted and continuous service delivery to customers.

100101 Service Continuity Plan

Business Continuity Management (BCM) should be developed to determine a holistic approach taken to maintain service continuity.

This is to ensure that there is no disruption to processes in the provision of organizational services. This plan must be approved by Management.

The following should be noted:

a. Identify all emergency or recovery responsibilities and procedures.

b. Identify events that may interfere with business processes along with the potential and impact of such interruptions as well as the consequences of ICT security.

c. Implementing emergency procedures to enable recovery to be done as soon as possible or within the prescribed time frame.

d. Documenting processes and procedures that have been agreed.

e. Do a backup.

f. Test and update plans at least once a year.

RMCD

BCM planning should be developed and should contain the following:

a. List of core activities that are considered critical in the order of priority.

b. List of LTAT and vendor personnel together with contactable numbers (facsimile, phone and email). The second list should also be provided as replacing personnel unable to attend to address the incident.

c. Complete list of information that requires backup and actual storage location as well as instructions for restoring information and related facilities.

d. An alternative source of processing and location to replace a lumped source.

e. Agreements with service providers to get the service reconnection priority where possible.

A copy of the BCM plan should be kept in a separate location to avoid catastrophic damage in the main location. The BCM plan should be tested at least once a year or when there is a change in the environment or business function to ensure it remains effective. Evaluation should be regularly conducted to ensure that the plan is appropriate and meets the intended purpose. BCM plan tests should be scheduled to ensure that all members in the recovery and personnel involved are aware of the plan, their responsibilities and roles when the plan is implemented. LTAT should ensure that copy of BCM plan is always updated and protected as in the primary location.	

ARTICLE 11 COMPLIANCE	
1101 Compliance and Legal Requirements	
Objective: Increase the level of ICT security to avoid violations of the LTAT Information Security Policy.	
110101 Compliance Policy	
Every user at LTAT shall read, understand and comply with the LTAT ICT Security Policy and other relevant laws or regulations in force. All ICT assets in LTAT include the information stored therein the ownership of LTAT. The Head of Department / authorized officer reserves the right to monitor the user's activity to detect the use other than the intended purpose. Any use of LTAT ICT assets other than the intended purpose and purpose, is a misuse of LTAT resources.	**All**
110102 Compliance with Policies, Standards and Technical Requirements	
ICTSO shall ensure that all safety procedures in their respective areas of work comply with policies, standards and technical requirements. Information systems need to be reviewed periodically to comply with ICT safety implementation standards.	**ICTSO**
110103 Compliance with Audit Requirements	
Compliance with audit requirements is necessary to minimize threats and to maximize effectiveness in the information system audit process. The audit requirements and any inspection activities on the operating system should be planned and agreed to minimize the probability of interruptions in the provision of services. Access to information systems audit equipment should be maintained and supervised to avoid abuse.	**All**
110104 Legal Requirements	
The list of laws and regulations that all users of LTAT must follow is as in **Appendix 2**.	**All**
110105 Policy Violation	
Violation of the LTAT Information Security Policy may be subject to disciplinary action.	**All**

Effective Date:

This policy is effective from its date of production.

Puan Nik Amlizan Mohamed

Chief Executive
Armed Forces Fund Board

Date : 15/7/19

Appendix 1

DECLARATION OF CONFORMITY
LTAT INFORMATION SECURITY POLICY

Name (Uppercase) : ……..…….....……

No. Identification Card: …….....…….....

Position : …….....

Department : .....…….....

It really is and I actually confess that :-

1. I have read, understood and agreed upon the provisions contained in the LTAT Information Security Policy.

2. If I do not comply with the prescribed provisions, then the appropriate action may be taken on me.

Signature : .....

Date : .....

Confirmation of ICT Security Officer

.....
(Name of ICT Security Officer)
On Behalf : Chief Executive of LTAT

Date: .....

Appendix 2

LIST OF LEGAL AND REGULATORY

1. The Armed Forces Fund Act.
2. LTAT Financial Regulations.
3. Rules of Conduct.
4. Security Instructions.
5. General Circular No. 3 Year 2000 - Government Information and Communications Technology Security Policy Framework.
6. 6. General Circular No. 1 Year 2001 - Information and Communication Technology Incident Reporting Mechanism (ICT).
7. Public Administration Development Circular Number 1 Year 2003 - Guidelines on the Use of Internet and Electronic Mail at Government Agencies.
8. General Circular Letter Number 4 Year 2006 - Public Sector Information and Communication Technology Incident Management Handling Management (ICT).
9. Digital Signature Act 1997.
10. Official Secrets Act 1972.
11. Computer Crimes Act 1997.
12. Copyright Act (Amendment) of 1997.
13. Communications and Multimedia Act 1998.
14. General Commandments.
15. Treasury instructions.
16. Information Technology Directive 2007.
17. Personal Data Protection Act 2010.