A*STAR
Agency for
Science, Technology
and Research

CREATING AN INNOVATION ECONOMY

A*STAR
IT Security Policy
V1.1

TABLE OF CONTENTS

Annexes

A*STAR IT Security Policy

Version History

<table>
<tr><th>Ver. No</th><th>Ver. Date</th><th>Prepared by</th><th>Reviewed by</th><th>Approved by</th></tr>
<tr><td rowspan="2">1.0</td><td>18 Mar 15</td><td>David Koh</td><td>Nancy Chan, DD</td><td>John Kan, CIO</td></tr>
<tr><td colspan="4">Initial version.</td></tr>
<tr><td rowspan="3">1.1</td><td rowspan="2">16 Jul 15</td><td rowspan="2">Yap Soon Seong,
David Koh</td><td>Nancy Chan, DD</td><td>John Kan, CIO</td></tr>
<tr><td>Signature</td><td>Signature</td></tr>
<tr><td colspan="4">Changes
a) Reordered IT Acceptable Use Policy from Annex L to Annex N.
b) Revised IT Acceptance Use Policy and integrated the relevant policies into various Annexes.
c) Removed Annex M (Bring Your Own Device) and integrated the relevant policies into various Annexes.
d) Reordered Cross Border Travel Guide from Annex N to Annex L.
e) Reordered Security Awareness &amp; Training from Annex O to Annex M.</td></tr>
</table>

Page intentionally left blank

1 INTRODUCTION

1.1 Purpose

1.1.1 IT systems are critical and important assets of Agency for Science, Technology and Research (A*STAR). Without reliable and properly secured information and IT systems, A*STAR may not be able to carry out its mission. As such, appropriate steps must be taken to ensure that A*STAR IT systems are adequately protected from a variety of threats.

1.1.2 This document describes ways to prevent and respond to a variety of threats to IT systems including unauthorised access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use. It also serves to establish management direction, procedures and requirements to ensure protection of A*STAR information assets.

1.1.3 To ensure that the protection mechanism remains effective, reviews of risks to A*STAR information and IT systems must be conducted regularly.

1.1.4 To be effective, IT security must be a team effort involving the participation and support of every A*STAR staff and authorised personnel (such as contractors). In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users as well as steps they must take to help protect A*STAR corporate information and IT systems.

1.2 Policy Statement

1.2.1 A*STAR recognises the criticality and sensitivity of its information and IT systems. A*STAR management has a duty to preserve, protect, and account for A*STAR information.

1.2.2 It is the responsibility of **Whole of A*STAR (WOA)** staff to take due care to properly protect the confidentiality, integrity and availability of corporate information from unauthorised disclosure, modification, or destruction, and never to knowingly put A*STAR information or IT systems at unnecessary risk.

1.2.3 A*STAR information and IT systems must be protected in a manner that commensurate with its sensitivity and criticality. Access to A*STAR IT system shall be based on business needs.

1.3 Objectives

1.3.1 The objectives of this policy are:

- To establish a framework to maintain the confidentiality, integrity and availability of A*STAR information assets and IT systems,

- To ensure that the business is able to withstand threats to its information technology (IT) environment,

- To minimise the possibility of a threat to IT security causing loss or damage to the organization,

- To minimise the extent of loss or damage from an IT security breach or exposure,

- To ensure that adequate resources are applied to implement an effective IT security program,

- To identify the essential measures of the IT security program,

- To inform all personnel of their responsibilities and obligations with respect to IT security,

- To ensure that the principles of IT security are consistently and effectively applied during the planning and development of business activities.

1.4 Scope

1.4.1 This policy is applicable to WOA staff, and personnel who are authorised to access or use Government / A*STAR Corporate resources.

1.4.2 This policy applies to Government / A*STAR IT resources accessed by WOA staff and approved personnel. Corporate information represents any data contained in a corporate data system or any A*STAR-created materials. A*STAR-created materials include reports, emails, memoranda, or other materials created by an individual and used to perform business activities or to support management decision-making.

1.5 Definitions

For the purpose of understanding the policy, the following terminologies are used:

- “Personal Computers” or “Computers” refers to desktop computers, laptops, tablets, handheld devices, smartphones, wearables, external storage media, and any other end-users’ electronic devices that can be used to access A*STAR Corporate resources, regardless of whether these devices are issued by A*STAR.

- “Staff” refers to WOA staff (including permanent, contract and temporary staff).

- “Users” refers to staff and authorised personnel (including contractors and consultants) who have been given the rights to access A*STAR Corporate resources.

- All policies pertaining to “Staff” shall also apply to “Users”.

2 ROLES & RESPONSIBILITIES

2.1 A*STAR Information Technology Steering Committee

2.1.1 The overall guidance, direction and authority for information security is the responsibility and charter of the A*STAR Information Technology Steering Committee – chaired by the MD, with members comprising of DMD, EDs and Directors from the various divisions / departments.

2.1.2 The A*STAR Information Technology Steering Committee (ITSC) is overall responsible for:

- Providing leadership and strategic direction for the proper planning, budgeting, development and management of A*STAR IT systems and infrastructure;
- Introducing and driving holistic initiatives to enhance IT security;
- Approving A*STAR IT policies and any deviations from these policies;
- Approving security review, policy compliance, audits and risk assessment reports;
- Approving A*STAR Technical Architecture;
- Recommending disciplinary actions against errant staff.

2.2 Chief Information Security Officer (CISO)

2.2.1 The Chief Information Security Officer is responsible for providing advice on all security matters and for overseeing the execution of all security initiatives.

2.3 IT Security Team

2.3.1 IT Security Team is responsible for:

- Carrying out the day-to-day IT security activities;
- Central coordination for IT security activities;
- Establishing and maintaining organization-wide IT security policies, standards, guidelines, and procedures;
- Reviewing, monitoring and investigating IT security incidents;
- Advising project teams on IT security matters;
- Monitoring changes in the exposure of information assets to major threats;
- Defining and directing security initiatives and activities that can improve the implementation of security in A*STAR;
- Reviewing the security health of Critical IT Systems.

2.4 System Owner

2.4.1 System owners or their delegates are responsible for the acquisition, development, and maintenance of applications and systems that process A*STAR information. All applications or systems must have a designated system owner.

2.4.2 System owners are responsible for:

- Classification of the system or information;
- Conducting a Business Impact Analysis to determine the level of potential security impact that could affect the system. For Critical IT Systems, the owners are responsible for conducting further detailed risk assessments to determine the necessary mitigating controls.
- Defining which users will be granted access, and how the information will be utilised.

2.5 Users

2.5.1 Users are responsible for:

- Complying with the IT Acceptable Use Policy;
- Reporting IT security incidents to the IT Security Team;
- Using the information and systems only as authorised and intended by the system owners;

- Using strong passwords to protect access to information systems and resources.

2.5.2 All IT resources and Computers are to be used for work purposes only.

2.6 Application Services Team

2.6.1 Application Services Team is responsible for:

- Ensuring that applications and systems are developed with the necessary security measures;
- Implementing access control systems to prevent inappropriate information disclosure;
- Adhering to the Application Development and Maintenance Security Policy as well as other relevant security policies, standards and procedures;
- Testing the security controls implemented for adequacy, before putting the system into production.

2.7 Technical Services Team

2.7.1 Technical Services Team is responsible for:

- Ensuring that periodic security checks are carried out on the infrastructure, network and systems;
- Adhering to the Operations Management Policy and other relevant security policies for handling any request for changes to the operating environment;
- Ensuring that the operations, maintenance and disposal of systems are carried out securely according to the relevant security policies, standards and procedures;
- Making back-ups so that important information will not be lost;
- Ensuring that the systems are configured according to the A*STAR platform-specific secure configuration standards;
- Ensuring that the system and application logs are reviewed according to the Monitoring and Audit requirement in the Logical Access Control Policy.

3. DOMAIN-SPECIFIC POLICIES

3.1 The following are specific policies that make up the overall information security policy. In order to keep this document succinct and readable, the details are found in the Annexes.

a) **Application Development and Maintenance Security Policy (Annex A)**
This policy contains the security controls that application development staff needs to implement in order to develop secure applications and systems.

b) **IT Disaster Recovery Plan Policy (Annex B)**
This policy states that IT disaster recovery plan must be developed for Critical IT Systems, and that they must be reviewed and tested periodically.

c) **Configuration and Software Management Policy (Annex C)**
This policy ensures that all network and system environments are controlled, and that changes are properly reviewed and approved.

d) **Operation Management Policy (Annex D)**
This policy describes the overall policy for Data Centre Operations.

e) **Personal Computer Security Policy (Annex E)**
This policy gives instructions on how staff are to maintain the security of the Personal Computers and the information they contain.

f) **Information Classification and Handling Policy (Annex F)**
This policy describes how information assets in the IT systems shall be classified and handled.

g) **Internet and Intranet Policy (Annex G)**
This policy gives instructions on how staff are to ensure that the security of A*STAR information and systems are not compromised while using the Internet.

h) **Email and Instant Messaging Policy (Annex H)**
This policy gives instructions on how staff are to ensure that the security of A*STAR information and systems are not compromised while using the Email and Instant Messaging.

i) **Network Security Policy (Annex I)**
This policy governs the proper use of A*STAR IT network, both wired and wireless.

j) **Logical Access Control Policy (Annex J)**
This policy dictates the logical access control for staff, equipment and the log review requirements.

k) **Personnel and Physical Security Policy (Annex K)**
This policy contains the instructions for security clearance of personnel during hiring. It also includes the measures to ensure that the physical security of offices and computer systems is protected.

l) **Cross Border Travel Guide (Annex L)**
This document provides guidance to staff who are travelling overseas with devices containing sensitive data.

m) **Security Awareness & Training (Annex M)**
This policy states the requirements for A*STAR security awareness and training programme

n) **IT Acceptable Use Policy (Annex N)**
This policy highlights the key IT security policies that affect users. This document helps users to understand their roles and responsibilities pertaining to access and use of A*STAR IT resources.

4. DISCIPLINARY MEASURES FOR VIOLATIONS

4.1 A*STAR reserves the right to monitor computer facilities, systems, files etc for any suspected abuse, unauthorised or illegal activities with approval of the CIO and the relevant functional heads.

4.2 Staff who deliberately violate this and other information security policies are subject to disciplinary action including termination.

4.3 In addition, staff are warned that violations and misuse of computer systems could also result in legal prosecution by the Singapore Government, under the Computer Misuse and Cyber security Act.

5. INCIDENT REPORTING

5.1 All suspected policy violations, system intrusions, virus infections, and other conditions which might jeopardise A*STAR information or A*STAR information systems must be immediately reported to the IT Security Team through the IT Helpdesk.

6. DEVIATION

6.1 All deviations from this policy and the supporting documents will have to be submitted for approval by the A*STAR Information Technology Steering Committee.

7. POLICY REVIEW AND AUDIT

7.1 This policy and the supporting policies, standards and procedures shall be reviewed at least once every 12 months, to ensure it remains relevant for A*STAR and aligns with our changing environment.

7.2 Audit shall be carried out by the Internal Audit Department on critical systems, as defined in Business Impact Analysis, once in every 2 years.

A APPLICATION DEVELOPMENT AND MAINTENANCE SECURITY

1 Introduction

1.1 The purpose of this section is to ensure that the security is built into the information system.

2 Application Security

2.1 System owners must specify the security requirements in the design of their applications.

3 Risk Management

3.1 Risk Management must be carried out for IT application above $500K, according to the ICT Risk Management Methodology.

4 Security Requirement of Systems

4.1 Business requirements of new systems or enhancements to existing systems shall include the requirements for security control.

4.2 Data input to application shall be validated to ensure that it is correct and appropriate.

4.3 Validation checks shall be incorporated into systems to detect corruption of data processed.

4.4 Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.

4.5 Data output from application shall be validated to ensure that processing of stored information is correct and appropriate to the circumstances.

4.6 Reports generated shall include protective markings as appropriate to the classification of the information that is generated.

4.7 Periodic tests shall be conducted on the systems to detect security vulnerabilities and ensure that the security controls are effective.

4.8 Source code review shall be conducted before the internet-accessible Application System is deployed or upon source code changes.

4.9 Penetration testing shall be conducted on internet-accessible Application Systems as stipulated below:

Type	Prior to Deployment	Upon Major Changes	Annually
Internet-accessible Application Systems	Yes	Yes	Yes

4.10 Vulnerability scanning shall be performed on all internet-accessible Application Systems and Critical IT Systems. The application software, operating system and network infrastructure shall be scanned according to the frequency stipulated below:

Component	Frequency
Application Software	Yearly
Operating System	Quarterly
Network	Quarterly

4.11 Measures to ensure timely detection of defacement and recovery of internet-accessible Application Systems shall be implemented.

4.12 Security patches shall be implemented according to the timeframe stipulated below:

Type of System	Type of Patch	Deployment upon availability of Patch
All	Emergency	24 hours
a) Critical IT Systems b) Internet-accessible Application Systems c) Service-Wide Systems and Infrastructures	High	2 weeks
	Medium / Low	6 weeks
Intranet Application Systems	High	4 weeks
	Medium / Low	12 weeks

4.13 Measures shall be implemented to ensure that classified information is securely erased from storage media prior to the media re-deployment, repair or disposal. The erasure method used shall not allow a reconstruction of the data stored on the media.

5 Cryptographic Controls

5.1 Encryption is required to protect sensitive and proprietary data that would otherwise travel over untrusted public or private links.

5.2 Encryption shall be applied to protect the confidentiality of sensitive or critical information.

6 Security of System Files

6.1 Controls shall be applied to the implementation of software in all environment.

6.2 All environment shall be protected and controlled.

6.3 Strict control shall be maintained over access to programs.

B IT DISASTER RECOVERY PLAN

1 Introduction

1.1 The purpose of this section is to ensure that A*STAR can continue its activities in the event of major failures or disaster.

2 Management Responsibility

2.1 The ITSC shall support and commit sufficient resources for the development, testing and on-going maintenance of IT Disaster Recovery Plan (DRP).

2.2 The responsibility and authority for the creation, testing, review and update of the IT DRP shall be defined and assigned.

3 DRP Operation

3.1 Each identified critical system and application must have a DRP.

3.2 DRP shall define the essential levels of service and the maximum acceptable periods of down-time for critical information processing systems.

3.3 DRP must be documented and tested annually for Critical IT Systems.

3.4 DRP must be reviewed yearly for relevance and adequacy.

3.5 DRP must state clearly:

a) Definition of a disaster
b) Condition for the activation of the plan
c) Person(s) responsible for decision making during the crisis
d) Roles and responsibilities for each component of the plan during the crisis
e) Organization of the recovery team
f) Return to regular normal operations.

C CONFIGURATION AND SOFTWARE MANAGEMENT

1 Introduction

1.1 Configuration and software management ensures that a change process shall not disrupt the business processes.

2 Infrastructure Configuration Management

2.1 The configuration of system infrastructure such as switches, servers, routers and other IT devices shall be documented and validated.

2.2 Any changes to the configuration will be reviewed, tested and documented before they are applied.

3 Change Control

3.1 Changes to application and system configuration shall be made through migration and system change request form respectively. Custodians are responsible to maintain change controls of applications and system on behalf of the system owners.

3.2 Authorisations for changes shall be obtained from system owners.

3.3 System owners and users will be notified of all changes made to production system that may affect the processing data.

3.4 All user acceptance tests shall be performed in a controlled environment and will include, but not limited to:
a) Test Plan
b) Acceptance Test Criteria
c) Test objectives.

4 Use of Data for User Acceptance Testing Purpose

4.1 All software changes shall be tested in a UAT environment that replicates the production systems as close and practical as possible.

4.2 While the test data should be as close as possible to the live data, the use of live data containing sensitive information is to be avoided.

4.3 If data is to be used for testing purposes, the following rule applies:
a) Live data must be masked.

b) System owner shall authorise whenever live data is copied to the test environment.

c) Live data shall be properly destroyed after the testing is completed.

5 Unauthorised Software

5.1 Unauthorised software shall not be kept and installed on A*STAR network.

5.2 A list of authorised software shall be maintained. Any request to install unauthorised software shall be approved by the CIO.

6 Software Piracy

6.1 The making or use of unauthorised software copies is not permitted under any circumstances.

6.2 Staff will comply with all licensing terms and conditions regarding the use of any acquired software.

7 Computer Viruses

7.1 All computers shall be installed with the latest version of the anti-virus software and operating system patches/software patches before connecting to the network. The anti-virus software must be approved by A*STAR. The viral detection must be memory resident and enabled at all times. Anti-virus definition must be updated on a regular basis (at least weekly).

7.2 Staff shall scan files received from external sources before opening them.

7.3 A scan for computer viruses shall be conducted before and after maintenance or repair work has been done on computers and servers.

7.4 All computers and servers received from external source shall be scanned before connecting to the network.

D OPERATION MANAGEMENT

1 Introduction

1.1 The purpose of this section is to ensure correct and secure operation of A*STAR Data Centre.

2 Operational Procedures

2.1 All operating procedures shall be documented and maintained.

2.2 Changes to information processing facilities and systems shall be controlled.

2.3 Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.

2.4 Development and testing facilities shall be separated from the operational facilities.

2.5 Prior to using external facility management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into the contract or Service Level Agreement (SLA).

3 System Planning and Acceptance

3.1 Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

3.2 Acceptance criteria for new information systems, upgrades and new versions shall be established.

3.3 Suitable tests of the system must be carried out prior to acceptance.

4 Protection against Malicious Software

4.1 Detection and prevention controls to protect against malicious codes shall be implemented.

4.2 All computers shall be equipped with up-to-date detection software.

4.3 Procedures shall be established to guide the staff on the necessary actions if a malicious code has been detected or suspected.

4.4 Procedures shall be established to enable qualified staff to deal with such incidents.

4.5 Staff and third party vendors should be made aware of information security issues.

5 Housekeeping

5.1 Essential business information and system information shall be backed up regularly.

5.2 Backups shall be sent and stored at an off-site storage location on a timely basis, so as to ensure continued provision of the minimum essential level of service.

5.3 Backup procedures shall be documented, scheduled and monitored.

5.4 Backup procedures and retention periods shall be in accordance with the criteria approved by the System Owners and shall comply with legal/regulatory and user requirements.

5.5 Backup should be restored on a periodic basis for critical systems to test integrity and readability of the information stored.

5.6 A log of all storage and retrieval of off-site backups shall be maintained and periodically reviewed.

5.7 Staff's request for backup and restore of data residing in file server will be according to A*STAR backup and restore procedures.

6 Media Handling

6.1 Management of removable computer media such as tapes, disks, cartridges and printed reports shall be controlled.

6.2 Media shall be disposed of securely and safely when no longer required.

6.3 Media containing classified information shall be handled in accordance with A*STAR Information Classification and Handling Management Policy (Annex F).

6.4 System documentation should be accessible to authorised personnel only.

7 Exchange of Information and Software

7.1 To prevent loss, modification or misuse of electronic or manual exchange of information with other parties, agreements shall be established beforehand.

7.2 Media being transported shall be protected from unauthorised access, misuse or corruption.

7.3 There shall be a formal authorisation process before information is made public and the integrity of such information shall be protected to prevent unauthorised modification.

E PERSONAL COMPUTER SECURITY

1 Introduction

1.1 The Personal Computer Security Policy serves to govern the use of the personal computing environment in A*STAR to ensure the security of the hardware and software, and the appropriate handling and protection of A*STAR resources and interests. WOA staff and authorised personnel shall comply with this policy.

1.2 This policy establishes procedures and practices for the proper use and management of Personal Computers to process and store A*STAR data or gain access to A*STAR resources.

1.3 The terms “Personal Computers” and “Staff” are defined in the Introduction section of the A*STAR IT Security Policy.

2 Use Of Personal Computers

2.1 Personal Computers and peripherals, such as disk drives, are for official use only. They shall not be used for commercial activities or for personal gain. Staff shall be responsible for the proper usage of the equipment.

2.2 Staff shall not make any modification to the Personal Computer’s hardware, registry settings, built-in security features (e.g. jailbreak or rooting the device) and those applications installed by A*STAR.

2.3 Staff shall not install or use illegal or unauthorised software on the Personal Computers. Conversely, authorised software installed in the Personal Computers shall not be removed or disabled without prior approval from ITSS. Staff shall comply with the Copyright Act and Licensing agreements, where applicable (e.g. staff must stop using and uninstall the software after 30 days of evaluation; staff must not distribute the software beyond what is permitted).

2.4 Staff must report immediately to IT Helpdesk any incident of loss or theft, virus infection and tampering of sensitive information on the Personal Computers.

2.5 Staff shall scan all external storage media, such as CDs, DVDs, Thumb drives and external hard disks using the anti-virus software on the Personal Computers before using them.

2.6 Staff shall be accountable for the Personal Computers, the confidentiality of data residing within the system as well as the activities originating from the Personal Computers. In particular, staff shall not engage in any of the following activities:

a) Unauthorised access, disclosure, modification or destruction to A*STAR resources;

b) Using accounts or passwords assigned to others;

c) Attempting to circumvent security systems;

d) Attempting without authorisation, to exploit or probe for security holes in A*STAR or other organizations' networks / systems or engage in any malicious activities;

e) Attempting to degrade the performance of A*STAR or other organizations' networks / systems; and

f) Assisting other staff to cause damage to A*STAR or other organizations' networks / systems.

2.7 A*STAR has the right to access and disclose any data stored on the Personal Computers. Any request for access and disclosure of data stored on the Personal Computers has to be approved by the CIO and the relevant Functional Head.

2.8 Personal Computers shall be equipped with security control mechanisms, such as VPN and personal firewall.

2.9 Authentication tokens shall not be kept together with the Personal Computers.

2.10 Staff should turn off communication ports, Infra-Red, Bluetooth, GPS locator services, Near Field Communication (NFC), Data Roaming and Wi-Fi services on the devices when they are not in use to avoid any potential malicious attacks.

2.11 Sensitive data shall be securely erased in order to effectively remove the data from the Personal Computers.

2.12 Staff shall not use any non-A*STAR Personal Computers, network devices (such as switches, routers, hubs) or external devices (such as CD-ROM, DVD, Thumb drives, and external hard drives) to connect to A*STAR network or store A*STAR resources without prior approval from the CIO or designate.

2.13 For approved non-A*STAR Personal Computers, staff shall agree that A*STAR is not liable for any loss of data or software, or damages to the device resulting from its use to access the A*STAR networks, or to store or process A*STAR resources. Staff shall also agree to allow A*STAR to install, track, restrict access and monitor the use of the device.

F INFORMATION CLASSIFICATION AND HANDLING

1 Introduction

1.1 The purpose of this policy is to define the different classification of information assets in A*STAR and the required protection for the information in each classification.

2 Scope

2.1 Information assets refer to all information and data in hard copy or electronic form and software owned, used and administered by A*STAR. All information on A*STAR network that has not been identified as the property of other parties will be treated as A*STAR asset. Third-party information entrusted to A*STAR shall be protected according to applicable contractual agreements or official secret act.

2.2 All information assets used in A*STAR shall be classified and handled in accordance with this policy.

3 Classification of Information Assets

The information assets shall be classified as follows:

3.1 Unclassified

'UNCLASSIFIED' shall be applied to public domain information of which disclosure to people outside A*STAR has no impact to security.

Examples of information falling under this security classification include:

- Corporate Internet websites;
- Publicity emails;

3.2 Restricted

'RESTRICTED' shall be applied to information of which the unauthorised disclosure to people outside A*STAR will be UNDESIRABLE FOR ADMINISTRATIVE and SECURITY REASONS. These are other than those covered by higher security classifications, but still require security protection.

Examples of information falling under this security classification include:

- Orders, instructions, manuals etc not assigned to a higher classification but contain information which must not be communicated to the public without official authorisation;
- Training films and documents, manuals etc intended for official use and must not be released to the public;

This is the default classification for all information assets.

3.3 Confidential

'CONFIDENTIAL' shall be applied to information of which the unauthorised disclosure could be expected to CAUSE DAMAGE TO A*STAR or NATIONAL SECURITY.

Examples of information falling under this security classification include:

- Reports on operations and exercises that do not contain information of vital interest to a foreign country;
- Allocations of military and law enforcement radio frequency;
- Aerial photographs of Singapore other than those relating to important defence establishments or installations;
- Information disclosed to A*STAR by external parties under non-disclosure agreement.

3.4 Secret

'SECRET' shall be applied to information of which the unauthorised disclosure could be expected to CAUSE SERIOUS DAMAGE TO A*STAR or NATIONAL SECURITY.

Examples falling under this security classification include:

- Proposal for new schemes, the foreknowledge of which will prejudice their operation;
- Knowledge concerning foreign countries, the value of which depends upon the country concerned not knowing we possess them;
- Plans for the defence of areas other than vital strategic areas including details of associated operations, projected or current;
- Contingency plans for the maintenance of essential public services in event of an emergency;
- Adverse reports on general morale that will prejudice critical operations.

3.5 Top Secret

'TOP SECRET' shall be applied to information of which the unauthorised disclosure could be expected to CAUSE EXCEPTIONALLY GRAVE DAMAGE TO NATIONAL SECURITY. The circulation of 'TOP SECRET' information should be confined to designated senior officers of A*STAR.

Examples of information falling under this security classification include:

- Defence policy or plans;
- Policy plans or details of major operations, projected or current, for the defence of strategic areas or vital installations;
- Information on the methods used or success attained by Singapore or allied intelligence and security services and information that will endanger special agents;
- Critical information on major scientific and technical developments.

4 Data Access and Ownership

4.1 The Data Owner is responsible for the integrity and confidentiality of the data.

4.2 All individuals accessing the data are required to protect the data according to the measures stated in this document.

4.3 Access to classified data should be on a need basis.

4.4 All data access rights of individuals should be reviewed periodically or when there are changes in the appointment/role of an individual.

5 Handling of Security-Classified Information

Staff shall be familiar with the necessary processes and procedures with regard to handling of sensitive documents or data.

5.1 Unclassified

Such data may be released to others without prior approval.

5.2 Restricted

Such data may be distributed or copied within A*STAR but not released to the general public.

For information assets classified Restricted and above, the distribution of such information shall be based on need-to-know basis and authorisation from data owner is required. Release of such information to authorised external parties must be done under non-disclosure agreement.

Disclosure of information of security classification Restricted and above to third party without proper authorisation is an offence and is subject to disciplinary or legal action.

All removable storage media containing information of security classification Restricted and above shall be secured in locked cabinets when not in use.

Information of security classification Restricted and above may be stored on hard disks only if an access control software and/or authorised encryption software is used to protect the data.

5.3 Confidential

For information assets classified Confidential or below, usage of cryptographic modules is encouraged to protect the confidentiality of the electronic data in storage or in transit. It shall be mandatory if A*STAR deem that a breach in confidentiality would be detrimental to the reputation and public image of A*STAR.

For electronic data that are classified Confidential and above, which is stored on a centralised server, all access should be logged.

5.4 Secret & Above

For information assets classified Secret & above, usage of cryptographic modules is mandatory to protect the confidentiality of the electronic data in storage or in transit.

All storage media containing information of security classification Secret and above must NOT be subject to repair by vendor.

No Secret & above data or information shall be stored or handled by current A*STAR IT systems.

6 Information Retention

6.1 For all electronic data that are classified as Restricted and above, the Data Owner shall determine the record retention period.

6.2 Data Retention Period Table

Type of Data	Retention Period
HR Data • Payroll, Personnel, Claims, Training, Leave, Medical records	10 Years
Finance Data • Payment, Point of Sales (if any), Inventory, Fix Assets records	10 Years
Administrative Data • Minutes of Meetings, EXCO Reports	10 Years
Patents Records • Technology Disclosure, Patent Document	20 Years
Legal Agreements • RCA, License Agreement, Consortium Agreement, NDA	10 Years
Research Data	10 Years
Scholars Data	20 Years

7 Disposal of Electronic Data

7.1 Approval & Recording

All disposal of electronic data or information classified as Restricted and above shall be approved by the Data Owner.

Disposal of all electronic data classified as Confidential and above must be recorded.

7.2 Secure Erasure

Secure Erasure, also known as sanitization refers to the process of erasing, as far as possible, the data on storage media to minimise the risk of a successful data recovery, particularly the reconstruction of security-classified information by unauthorised personnel which can lead to embarrassment to A*STAR.

There are 3 common methods of secure erasure:

a) Overwriting – This is a software procedure of replacing previously stored data with a predefined set of meaningless data.

b) Degaussing – This is a hardware procedure (appliance-based) to demagnetise magnetic storage media to purge its contents. This method is more effective and faster in securely erasing the data than the overwriting method. However, the process usually renders the storage media unusable.

c) Physical Destruction – This annihilates the physical form of the storage media and includes techniques such as disintegrator, burning, wet pulping, chemical decomposition and pulverising.

For disposal of all electronic data classified as Confidential and below, A*STAR at its own discretion, shall assess and manage the security risk involved by selecting the most appropriate secure erasure method (i.e. overwriting, degaussing or physical destruction).

For disposal of all electronic data classified as Secret and above, overwriting/degaussing method shall be used, followed by physical destruction.

G INTERNET AND INTRANET

1 Introduction

1.1 The Internet / Intranet are widely used by staff as a source of information and means of communication.

2 Use of Internet / Intranet

2.1 Staff shall use Internet / Intranet resources for official purpose only.

2.2 Staff shall ensure that all files downloaded from the Internet are scanned using the virus scan software provided by A*STAR.

2.3 Material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance or is otherwise unlawful or inappropriate must not be sent by email or other forms of electronic communication such as bulletin board systems, newsgroups, mailing lists and chat groups. Such material should not be downloaded from the Internet, displayed on or stored in computers.

2.4 Staff shall not be involved in activities that waste or misuse A*STAR computing resources. These activities include, but are not limited to, sending unauthorised mass emails, electronic chain letters or engaging in online chat groups for personal purposes.

2.5 Materials posted on the Internet may be copyrighted. Staff shall seek permission from the author before copying and using the material.

3 Monitoring of Internet / Intranet and Handling Inappropriate Content

3.1 A*STAR has the right to monitor any and all aspects of Internet / Intranet usage & resources, including, but not limited to, sites visited by staff, chat groups, bulletin boards, mailing lists and newsgroups participated by staff.

3.2 A*STAR has the right to block staff from accessing any web sites that are deemed to be unlawful or inappropriate.

3.3 Staff shall report any incident of receipt of undesirable materials that are obscene or harassing in nature.

4 Security

4.1 Staff shall not use the Internet / Intranet to gain unauthorised access to any computer systems that are connected to the Internet / Intranet.

4.2 Where an ID is required to access Intranet / Internet services, the staff shall use his own ID.

4.3 Staff shall not deliberately introduce any form of computer viruses while using the Internet / Intranet services.

4.4 Staff shall enable security settings (such as SSL or TLS) in web browsers.

4.5 Staff shall clear their web browser cache upon exit.

H EMAIL AND INSTANT MESSAGING

1 Introduction

1.1 Electronic mail (or e-mail) is transmission of messages (which includes text, graphics, data, audio visual clips and web links) from computer to computer via a communications network. It is used on both local area networks (LAN) and or larger communications networks (e.g. Internet). Because of its fast speed and relatively cheap cost of usage, e-mail is increasingly used to transmit official business messages, thus replacing traditional modes of communication (e.g. letter, minute, fax).

1.2 Instant Messaging (or IM) is also another transmission of messages (includes text, web links, attachment and multi-party conferencing) from computer to computer via a communications network for collaboration. However, instant messaging does not have digital signing and logging features. Hence, IM could not provide non-repudiation needs.

2 Security Classification

2.1 Information and materials are graded according to 5 categories – Unclassified, Restricted, Confidential, Secret and Top Secret.

2.2 When handling and sending mail, staff should be aware of the classification of the information and handle it in accordance with A*STAR Information Classification and Handling Management Policy (Annex F).

2.3 Staff shall adhere to the use of the following mail systems when sending mail with the following classification:

Classification	**SG-Mail or A*STAR Email**	**SG-Mail Secure**	**Other Mail system & Instant Messaging**
Unclassified	Yes	No	Yes
Restricted	Yes	Yes	No
Confidential	Yes, with discretion	Yes	No
Secret	No	Yes	No
Top Secret	No	No	No

2.4 Highly classified documents i.e. TOP SECRET shall not be transmitted using e-mail and instant messaging.

2.5 Mail contents that are classified as SECRET shall be encrypted during the transmissions from point to point and staff shall ensure that only approved secure email system is used to transmit and store the email.

2.6 Staff shall exercise his / her discretion when deciding whether CONFIDENTIAL or RESTRICTED information can be transmitted through the mail system without encryption.

2.7 As the mail sent via Internet are transmitted through mail servers that are outside A*STAR's purview, staff shall note the security vulnerabilities of Internet mail and not send mail with contents that may compromise the integrity and privacy of the individual and the department. This includes mail with the following content:

a) Sensitive Government / A*STAR information such as strategic plans, personnel matters and finances;

b) Account or authentication information that would allow someone to breach security of a given account or ID;

c) Information pertaining to internal security practices or breaches;

d) Sensitive personal data which intrudes on a person's privacy.

3 Official Correspondence

3.1 Staff can use the Government / A*STAR mail systems mentioned in this policy to transmit information and communicate official decisions. If there is a need for non-repudiation, staff shall ensure that the e-mail or attachments are digitally signed, logged or otherwise rendered non-editable through the use of appropriate software.

3.2 Public Internet mail, such as Yahoo or Hotmail, shall not be used for official internal correspondences. A*STAR entities which receive queries and feedback from Internet mail can respond officially using the same medium. However, Internet mail without authentication shall not be used as the sole medium for official correspondences which may subsequently be used by A*STAR entities as evidences, for example in contract negotiation and agreements.

4 Ownership of E-Mail and Instant Messaging

4.1 Messages that are created, sent or received using the Government / A*STAR's e-mail and instant messaging systems are the property of the Government / A*STAR.

4.2 A*STAR has the right to access and disclose any information found in the system. Any request for access and disclosure of user email messages has to be approved by the CIO.

5 Misuse of Email and Instant Messaging

5.1 A*STAR entities / departments are responsible for informing their staff on the proper use of the Government / A*STAR e-mail and IM systems, and to take the necessary action in the event of violation of this policy. New staff in particular shall be informed of the proper usage of e-mails and IM, as soon as they join the organization.

5.2 Emails should be used with discretion so as not to compromise the integrity and privacy of the individual and A*STAR. Staff are responsible for the custody and transmission of their emails.

5.3 To prevent misuse, user identity and accountability must be established for all e-mail and IM, and enforced via unique ID and password for access.

5.4 Staff shall implement good password management practices in accordance with A*STAR password control policy. Staff shall not give their password to anyone and shall guard against the unintended disclosure of their password.

5.5 As e-mail and IM accounts are corporate resources, staff shall confine their use of electronic mail and instant messaging to official purposes, whether to other A*STAR staff or beyond.

5.6 Staff shall not misuse a given account or system. Misuse includes the following:

a) Using e-mail, IM or any broadcast media for purposes of defamation or personal attack;

b) Sending e-mails to the general public in a way that can be viewed as spamming;

c) Using e-mail, IM or any broadcast media to post potentially offensive information that would impinge on another's culture, ethics, morality and religion;

d) Send offensive or seditious material to other users, either within A*STAR or outside;

e) Obtain offensive or seditious material from the Internet;

f) Create and send advertisements, chain letters and other unsolicited type of messages;

g) Make private orders or other forms of private messages that may imply that the sender has taken on obligations;

h) Use the Internet facilities for personal gain or profit;
i) Make commercial solicitations including tontines and pyramid schemes for himself or for others;
j) Send unlicensed software and material that violates copyright laws;
k) Knowingly send a program intended to damage or place excessive load on a computer system or network. This includes computer viruses, Trojan horses and worms;
l) Attempt to circumvent data protection schemes or uncover security loopholes;
m) Masking the identity of an account or machine; and
n) Indiscriminate broadcasting of e-mail or IM through large distribution lists.

5.7 If user sends marketing e-mails to the general public, he shall:
a) Include in the e-mails a valid return e-mail address by which the sender can be readily contacted;
b) Mark unsolicited marketing e-mails as advertisements by inserting <ADV> in the subject line; and
c) Provide an electronic option in the e-mails so that recipients can remove themselves from the distribution lists for future e-mails and have processes in place to remove them promptly.

5.8 Misuse may be cause to terminate a given account, and can be the basis for disciplinary action. Depending on the nature and circumstances of the misuse, staff may be subjected to the laws and regulations such as Intellectual Property Rights and Computer Misuse Act.

5.9 User should not open attachments or links from unknown sources (e.g. phishing, scam, spamming e-mails, etc).

5.10 Any incident of misuse shall be reported to the IT Security Team.

I NETWORK SECURITY

1 Introduction

1.1 Network security covers the management and usage of internal and external network.

2 Internal Connectivity

2.1 All network devices, such as routers, switches, hubs, wireless AP devices, modems and other devices are to be managed and controlled by ITSS other than those on subscription.

2.2 Routers and switches must be configured to provide access control.

2.3 Only authorised network devices shall be connected to A*STAR network.

2.4 All unused ports not within the office vicinity should be disabled.

3 External Connectivity

3.1 An intrusion detection system must be in place to monitor for attacks in the network.

3.2 Any connection to external host / network must be approved by the CIO.

3.3 Sensitive information transmitted over unsecured network transmission media shall be encrypted.

4 Remote Access

4.1 Staff shall be aware of their responsibilities when accessing A*STAR resources and data outside the office, where the risks of security exposure are higher.

4.2 Remote access computers shall include, but are not limited to, the following security features:

a) Staff shall logon to the A*STAR network via an encrypted link.

b) Staff shall authenticate to the domain controller to join A*STAR network.

c) Remote computers shall be equipped with anti-virus software with the latest updates or patches.

d) Use of non-A*STAR Personal Computers to remote access back to A*STAR must be approved by the CIO or designate.

4.3 Remote access facilities (i.e. VPN appliance) for all computers or communication systems shall be properly secured from unauthorised access so as to protect the confidentiality and integrity of data.

4.4 Approval is required from ITSS if external contractors or collaborators need to access A*STAR network / resources.

5 Wireless LAN

5.1 Strong authentication mechanisms (i.e. VPN access) shall be used to prevent unauthorised access to internal network via WLAN.

5.2 Sensitive information transmitted over the WLAN shall be encrypted.

5.3 Access control mechanisms such as firewall shall be implemented to segregate WLAN from internal wired network. The WLAN shall be deployed in a different network segment by VLAN, which is separated from internal wired network.

5.4 Broadcast of ESSID/SSID shall be turned off on all active access points (AP) except for public-facing shared AP.

5.5 Wireless stations or access points shall be placed within A*STAR premises.

6 Network Usage

6.1 A*STAR networks (wired and wireless) are for official use only.

6.2 Staff shall not connect to multiple networks or configure their Personal Computer to access A*STAR networks and public network concurrently.

6.3 Staff shall use only A*STAR-approved hardware and software on A*STAR networks.

6.4 Only staff with an authorised account and password is allowed to access A*STAR network resources.

6.5 Staff shall not configure the devices to perform routing or offer network services such as DHCP service.

6.6 Staff shall not use any IP addresses that have not been assigned to their devices.

J LOGICAL ACCESS CONTROL

1 Introduction

1.1 The purpose of logical access is to manage access to information in a way that:

a) System is protected from unauthorised access.
b) Accidental damage from authorised personnel is minimised.
c) Staff has access to appropriate resources.

1.2 This section addresses the logical access control for staff and network devices such as routers, switches and computers.

1.3 Audit requirements are also addressed in this section.

2 Password Standard

2.1 The use of sign-on passwords must be implemented and passwords must not be displayed in clear.

2.2 Staff must protect password confidentiality from disclosure and compromise at all times.

2.3 Password must always be encrypted during transmission and in storage.

2.4 Strong passwords shall be chosen to minimise the risk of others guessing the passwords e.g. common names or dictionary words should not be used.

2.5 Passwords should be changed periodically (minimally every 90 days) or whenever the user suspects that the password has been compromised.

3 User Access Control

3.1 Staff shall have their own User IDs for the system they work with. User ID and password are personal and shall not be shared or disclosed to others.

3.2 Access rights to data stored in IT systems shall be approved by the respective system owners. Staff can request for access rights through the IT Helpdesk.

3.3 Staff shall sign the confidentiality agreement before they are registered on A*STAR systems.

3.4 There shall be a formal procedure for user registration and de-registration for multi-user information systems.

4 User Access Profiles

4.1 Every application must have a user access profile. System owners are responsible for authorising access to applications under their purview.

4.2 A formal record of all registered users and their access rights must be maintained.

4.3 Non-standard access may be granted in exceptional circumstances subject to authorisation and control. These exceptional circumstances shall apply only for a limited time.

5 Authentication and Password

5.1 Staff must be uniquely identified in the systems and shall be held accountable for every action carried using his/her User ID.

5.2 Staff must be identified and authenticated on the systems before being granted access.

5.3 Accounts shall adhere to the following settings:

a) Enforce password history – 5 passwords
b) Maximum Password Age – 90 days
c) Minimum password length – 8 alphanumeric characters, with at least 1 alphabet and 1 numeral
d) Account lockout threshold – 5 invalid logon attempts

5.4 User ID must be suspended if one of the following conditions applies:

a) User ID has not been used for a defined period[1] of time.
b) Termination of employment.

5.5 Suspended or inactive accounts must be deleted after a defined period of time.

[1] This clause is not applicable to SAP User ID due to the following reasons:

1. SAP User IDs held by senior management may be infrequently used.
2. There is a 6 monthly user access review by HR to flag out SAP User IDs that are no longer required by the organization.

6 Application Access Control

6.1 Access to application shall be restricted in accordance to the rules set by the system owners.

6.2 Regular review of accounts and associated access rights in the Systems shall be performed to ensure that unused or obsolete accounts and accesses are removed in a timely manner:

No	Type	Frequency
a.	Critical IT Systems	Quarterly
b.	Non-Critical IT Systems	Annual
c.	Inactive/Suspended Accounts	Monthly
d.	Staff who has left Agency, redeployed or changed job role	Monthly

6.3 Accounts and access rights review shall consider the following scenarios:

a) Staff Resignation/ Retirement
b) Termination
c) Transfer to another agency
d) Role change with same agency
e) Role change within same department
f) Extended leave
g) External Party User Resignation/Redeployment.

6.4 Systems and application services (such as web server services) shall be executed with limited access privileges.

7 Monitoring and Audit

7.1 Audit logs shall be retained at least one year so that investigation can be carried out when necessary.

7.2 Application and system audit trail shall be retained for a year.

7.3 Audit logs shall be protected against unauthorised access and corruption.

7.4 All computer clocks shall be synchronised on a regular basis. This is to ensure the accuracy of the audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

7.5 The following information must be captured in audit trail and monitored accordingly:

a) Successful and unsuccessful login event.
b) Security profile changes.
c) All activities related to privileged levels of access.

7.6 If there is no fixed or standard logging format available, the following minimum fields should be captured

a) Timestamp
b) User credential
c) Action taken

7.7 Audit logs must be readable in ASCII plaintext of UTF-8.

7.8 System and Application audit logs shall be reviewed on a regular basis.

K PERSONNEL AND PHYSICAL SECURITY

1 Introduction

1.1 Personnel security is required to minimise the risk of human error, theft, fraud, or misuse of the information system and its assets.

1.2 Human Resource Department shall take into account the security clearance required for staff who handles sensitive information.

1.3 Physical security and environmental control ensures the physical integrity and availability of system and network devices.

2 Confidentiality

2.1 Staff (including contracted vendors) shall be security cleared to the appropriate level, as determined by the designated owner, before being allowed to access the information assets or undertake IT projects.

2.2 Staff are responsible for protecting the confidentiality of the information assets under their custody. If deemed necessary, personnel (including contracted vendors) shall be required to sign a non-disclosure undertaking to protect the confidentiality of the information assets.

2.3 Before external parties are engaged to provide IT services for A*STAR, the security risks arising from the provision of the services shall be assessed and mitigated to an acceptable risk level.

2.4 Where external parties are engaged to provide services for the systems, the responsibilities of the external parties to comply with the security requirements shall be defined. Even if external parties are engaged to provide security services for the systems, the owners shall remain overall accountable for the security of their systems.

2.5 Computers holding sensitive information should only be accessible by authorised staff. Strong safeguard and authentication should be used.

2.6 Print-outs of classified documents must be collected immediately to prevent disclosure of information to unauthorised parties.

2.7 Staff shall not store or backup A*STAR confidential data to unapproved portable storage media (such as USB drive) and external cloud storage (such as Drop box, Google Drive, SkyDrive, Amazon Web Services, i-Cloud).

2.8 Staff shall ensure that auto-save to external cloud storage is disabled in devices and applications.

3 Data Centre

3.1 Critical IT equipment must be housed in a computer room to protect against vandalism and theft.

3.2 A data centre should be equipped with:
a) Proper fire detection and protection
b) Security alarm
c) Water detection system
d) Uninterruptible Power Supply / backup batteries

3.3 Access to the computer room is strictly for authorised personnel only.

3.4 Visitors to the computer room must be escorted by authorised personnel and are required to register entry and exit in the log book.

3.5 The security access logbook and/or card access logs must be reviewed regularly.

4 Cable Distribution Point

4.1 The communications equipment and cabling distribution points should be housed within lockable cabinets or rooms.

4.2 These areas are to be accessed by authorised personnel only.

5 Portable Storage Media

5.1 Portable storage media includes, but is not limited to, external hard disks, USB thumb drives, SD cards and built-in storage in hand held devices.

5.2 Portable storage media shall be used solely for work purposes only.

5.3 Staff shall only store their work related data on the approved Personal Computers’ hard disk, or shared drive facility/folder.

5.4 Staff can submit a request to ITSS to procure or issue additional portable storage media for scenarios such as:

a) Shared drive facility is not adequate;
b) Shared drive pose a constraint (e.g. connectivity issues);
c) External storage device is required for use by an individual for transfer of data, or for portability (e.g. for the individual's travelling or out of office meetings or demos/presentations);
d) External storage device is required for use by a department.

5.5 ITSS will review the request, before seeking CIO's approval to procure or issue any portable storage media to the department.

5.6 Head of Department shall be accountable for the management of the portable storage media issued by ITSS.

5.7 Staff are advised to handle the portable storage media with care while it is in their possession.
a) Portable storage media should be protected against theft (e.g. securely locked in cabinet) and not left unattended.
b) Portable storage containing classified data should only be accessible by authorised staff.

5.8 Staff shall ensure that confidential data is encrypted before it is stored on the portable storage media. If required, ITSS will provide the file encryption facility.

5.9 Staff leaving the organisation shall return the portable storage media to their Head of Department or immediate supervisor. When no longer required, the portable storage media shall be returned to ITSS.

5.10 In the event of loss of the portable storage media, staff shall notify their immediate supervisor and Head of Department, and submit the "Report on Loss of IT Equipment" form to ITSS.

6 Equipment Security

6.1 All IT equipment shall be located or protected to reduce the risks from environmental threat and hazards, and opportunities for unauthorised access.

6.2 Staff shall ensure that unattended equipment are protected from unauthorised use.

6.3 Critical equipment shall be protected from power failures and other electrical anomalies.

6.4 Cabling infrastructure shall be protected from interception or damage.

6.5 Third-party vendors should ensure the equipment brought in are free from malicious codes.

6.6 Equipment shall be maintained in accordance with manufacturer's instruction and/or documented procedures to ensure continued availability and integrity.

6.7 Staff shall not share computers with family, friends or others so as to prevent unauthorised access to A*STAR resources.

6.8 Staff shall not leave their accounts logged on when their Computers are unattended. Screen lock (e.g. via screen saver with access control) shall be activated after 10 minutes of inactivity.

6.9 Staff shall log out of IT systems/network and shut down their Computers at end of the day.

6.10 Computers must be protected against theft and should not be left unattended. Staff shall secure the computers to the desk or kept them away safely when not in use to prevent unauthorised access.

7 Maintenance

7.1 Measures shall be taken to reduce the risk of compromise of A*STAR systems and information during maintenance.

7.2 Only authorised personnel shall carry out IT equipment maintenance.

8 Repair and Servicing

8.1 Before sending the device for repair or servicing,

a) Staff shall change the password of the device to prevent the repair / service centre personnel from knowing the password.

b) Staff shall ensure that no corporate data is stored on the device.

8.2 Upon collection of the device from the repair / service centre,

a) Device password shall be changed immediately to prevent any potential unauthorised access to the device by the repair / service centre personnel.

b) Staff shall restore the device to factory default, in case malicious software, such as key logger, has been installed on the device.

9 Clean Desk Clear Screen Policy

9.1 Classified information in any form should not be left unattended. This includes information on papers or storage media left on the desk and information displayed on computer screen.

9.2 Desk should be cleared of classified information when not occupied.

9.3 Screen locks shall also be employed when inactivity has been detected on unattended computers unless work area, such as an office, can be locked.

10 Lost, Stolen or Compromised Equipment

10.1 In the event that any computer is lost or stolen,

a) Staff shall inform ITSS and make a police report in the respective country immediately;
b) Upon returning to work, staff shall submit an incident report, along with the police report to ITSS through IT Helpdesk;
c) If the loss of A*STAR-issued IT equipment is due to negligence, staff shall pay for the cost of repair or replacement of the IT equipment. The cost shall be determined by ITSS;
d) For handheld device, staff shall notify IT Helpdesk immediately and ITSS will secure wipe all corporate data in the device within 48 hours.

10.2 ITSS shall be allowed to conduct remote wipes on the device should ITSS find it to be compromised.

10.3 In the event of a suspected security breach, staff shall surrender the device to A*STAR for investigation. A*STAR will not be liable for any loss of data or software, or damages to the device due to the investigation.

11 Staff Leaving Organization

11.1 Upon leaving the organization, staff shall remove all corporate settings and data from the approved non-A*STAR devices.

L CROSS BORDER TRAVEL GUIDE

1 Introduction

1.1 This document provides guidance to staff who are travelling overseas with devices containing Government / A*STAR data.

1.2 To protect the security of their homelands, some countries have law empowering the custom officers to search, inspect and examine all persons, luggage and merchandise at their border controls. These cross border searches can include examining data on devices.

1.3 While staff are required to comply with the laws of the foreign countries, they are strongly encouraged to observe this Cross Border Travel Guide when travelling with devices containing Government / A*STAR data.

2 Guidance

2.1 The portable computing device (“device”) should only be hand-carried and not be checked in as check-in luggage.

2.2 The “device” should not be left unattended and should be within the line of sight of the staff at all times. If this is not possible, the “device” should be securely locked away.

2.3 At Immigration checkpoints, staff should be vigilant, holding on to the “device” until it is the staff’s turn to have his belongings X-rayed. Staff should keep an eye on the “device” while it is on the belt and ensure that it emerges on the other side of the X-ray machine.

2.4 If there is a request for the “device” to be searched/switched on, staff should ensure that all searches are done in his/her presence.

2.5 Staff should boot up and handle the “device” if requested by the Foreign Government Officer (FGO). Staff should not insert the PS Card or any other tokens which will allow access to sensitive materials stored in the “device”.

2.6 On no account should the staff allow the “device” to be taken away.

2.7 Staff may face the following scenarios:

a) An insistence by the FGO to take away the “device”.

b) An insistence by the FGO to connect external electronic devices to the "device".
c) Refusal by the FGO to allow the staff to depart if (a) or (b) are not complied with.

2.8 Should any of these scenarios be encountered, staff should politely but firmly raise objections. Staff should not aggravate matters by physically resisting but should: (a) ask for the FGO's name, and (b) ask to speak with the FGO's supervisor. Staff should explain to the supervisor that he is not at liberty to do as requested by the FGO as the access to the "device" or its data needs to be explicitly authorised. Should this fail, staff should insist on his right to consular access and seek assistance from:
a) The relevant Singapore Mission; or
b) The Ministry of Foreign Affairs.

2.9 The contact details of Singapore Missions and MFA's 24-hour duty office numbers for urgent consular assistance are available on MFA's website.

2.10 Staff should also keep A*STAR informed of the situation.

2.11 At no time should the staff take the path of least resistance and submit to the requests made.

3 Technical Measures

3.1 Staff should adopt the following technical measures to further minimise the risk of disclosure of classified information when travelling:

a) Encrypt the "device" or any portable storage media using A*STAR-approved software; or
b) Use a dedicated portable computing device for travelling such as a portable computer that does not store classified information on its local hard disk. Staff using the dedicated device should download the required security-classified information at the destination and securely erase all security-classified information from the device prior to return from the official business trip.

M SECURITY AWARENESS AND TRAINING

1 IT Security Awareness

1.1 An IT Security Awareness Program shall be implemented to educate staff on IT security risks and protection measures on a regular basis.

1.2 The awareness program will cover:

a) Security classifications of e-mail messages supported by the e-mail systems;

b) A*STAR e-mail policies that staff have to adhere to;

c) Authorised software allowed on Personal Computers.

2 IT Security Training

2.1 IT Security training shall be provided for staff who design, implement or maintain systems, regarding the types of security and internal control techniques that should be incorporated into system development, operations and maintenance.

2.2 Staff who are assigned with IT security responsibilities shall be provided with in-depth training regarding security techniques, methodologies for evaluating threats and vulnerabilities that affect specific IT systems and applications, and selection and implementation of controls and safeguards.

N IT ACCEPTABLE USE POLICY

The IT Acceptable Use Policy includes all the end-user clauses in the A*STAR IT Security Policy. It includes but is not limited to the following Annexes in the A*STAR IT Security Policy:

Annex C: Configuration and Software Management Policy
Annex E: Personal Computer Security Policy
Annex F: Information Classification and Handling Policy
Annex G: Internet and Intranet Policy
Annex H: Email and Instant Messaging Policy
Annex I: Network Security Policy
Annex J: Logical Access Control Policy
Annex K: Personnel and Physical Security Policy
Annex L: Cross Border Travel Guide

The A*STAR IT Security Policy is available in the KU (Knowledge Universe).
https://ku.a-star.edu.sg

Declaration

I have read the IT Acceptable Use Policy and will abide by it. I acknowledge that I am responsible for the proper use of A*STAR Corporate resources.

A*STAR reserves the right to amend the A*STAR IT policies without users' prior consent. I agree and will adhere to any future amendments of A*STAR IT policies.

Name: ____________________ **Signature:** ____________________

Entity/ Dept: ____________________ **Date:** ____________________