Information Security Policy

Table of Contents

History

Version	Date	Author	Summary of Changes
0.1	March 2015	Farah Datuk Rameli	- Draft
1.0	June 2015	Farah Datuk Rameli	- First issue
			-
			-

1.0 INFORMATION SECURITY MISSION STATEMENT

INGRESS and INGRESS employees have an inherent responsibility to protect the physical information assets of the company as well as confidential information data and intellectual capital owned by INGRESS. These critical assets must be safeguarded to mitigate any potential impacts to INGRESS and INGRESS's shareholders. Information Security at INGRESS is, therefore, a critical business function that should be incorporated into all aspects of INGRESS's business practices and operations.

To achieve this objective; policies, procedures, and standard guidelines, have been created to ensure secure business practices are in place at INGRESS. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

INGRESS is subject to numerous Federal Information Security and Privacy laws and regulations, which if not complied with, could potentially result in fines, audits, loss of shareholders confidence, and direct financial impacts to the company. Compliance with all applicable regulations is the responsibility of every employee at INGRESS.

2.0 OBJECTIVES AND PRINCIPLE

2.1 Information Security Principles

The policy introduces some generally accepted principles that address information security from a very high-level viewpoint. These principles are fundamental in nature, and rarely changing. They are NOT stated here as information security requirements but are provided as useful guiding references for developing, implementing and understanding information security policies. The principles listed below are by no means exhaustive.

2.1.1 Information security objectives

Information system security objectives or goals are described in terms of three overall objectives:

a. Confidentiality: Means that information is only being seen or used by people who are authorised to access it.

b. Integrity: Means that any changes to the information by an unauthorised user are impossible (or at least detected), and changes by authorised users are tracked.

c. Availability: Means that the information is accessible when authorised users need it.

Information Security policies and measures are developed and implemented according to these objectives.

2.1.2 Prevent, Detect, Respond and Recover

Information security is a combination of preventive, detective, response and recovery measures.

a. Preventive measures are for avoiding or deterring the occurrence of an undesirable event.

b. Detective measures are for identifying the occurrence of an undesirable event.

c. Response measures refer to coordinated response to contain damage when an undesirable event (or incident) occurs.

d. Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Information Security measures should be considered and implemented as appropriate to preserve the confidentiality, integrity, and availability of the information while it is being processed, in transit, and in storage.

2.1.3 Auditability and Accountability

Information Security requires auditability and accountability.

a. Auditability refers to the ability to verify the activities in an information system. Evidence used for verification can take form of audit trails, system logs, alarms, or other notifications.

b. Accountability refers to the ability to audit the actions of all parties and processes which interact with information systems. Roles and responsibilities should be clearly defined, identified, and authorised at a level commensurate with the sensitivity of information.

3.0 REFERENCES

3.1 Standards and Guidelines

a) ISO/IEC 17799:2000; Information technology – Security techniques – Information security management systems – Requirements,

b) ISO/IEC FDIS 27002:2013; Information technology – Security techniques – Information security management systems – Requirements,

c) National Information Assurance (IA) Glossary - CNSS Instruction No. 4009 – is an unclassified glossary of Information security terms intended to provide a common vocabulary for discussing Information Assurance concepts.

d) Online Technology glossary by - http://www.techopedia.com

4.0 DEFINITION AND CONVENTION

4.1 Terms and Definitions

Ref.	Item	Description
a.	INGRESS	Group of companies, which consist of Ingress Corporation Berhad, Ingress Industrial Thailand Co., Ltd, Ingress Industrial Malaysia, Ingress Auto Venture Co., Ltd, Ingress Technologies Sdn Bhd, Ingress Precision Sdn Bhd, Fine Component (Thailand) Co., Ltd, P.T. Ingress Malindo Ventures, Ingress Auto Sdn Bhd, Ingress Motor Centre Sdn Bhd, Ingress Fabricators Sdn Bhd, Multi Discovery Sdn Bhd, Ramusa Engineering Sdn Bhd, Talent Synergy Sdn Bhd, Ingress Engineering Sdn Bhd, Ingress Katayama Technologies Centre Sdn Bhd
b.	Information System	A related set of hardware and software organised for the collection, processing, storage, communication, or disposition of information.
c.	Confidentiality	Means that the information is only being seen or used by people who are authorised to access it.
d.	Integrity	Means that any changes to the information by an unauthorised user are impossible (or at least detected), and changes by an authorised users are tracked.
e.	Availability	Means that the information is accessible when an authorised users need it.
f.	Information Security Policy	a documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by information systems from any unauthorised disclosure, modifications or destruction.
g.	Classified Information	Refers to the categories of information classified in accordance with the Security Regulations.
h.	Staff	Persons employed by the INGRESS irrespective of the employment period and terms.
i.	Data Centre	A centralised data processing facility that houses Information Systems and related equipment. A control section is usually provided that accepts work from and releases output to users.
j.	Computer Room	A dedicated room for housing computer equipment.

k.	Malicious Codes	Programs intended to perform an unauthorised process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malicious codes include computer viruses, worms, Trojan horses, and spyware etc.
l.	Mobile Devices	Portable computing and communication devices with information storage and processing capability. Examples include portable computers, mobile phones, tablets, digital cameras, and audio or video recording devices.
m.	Removable Media	Portable electronic storage media such as magnetic, optical, and flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard disks or solid-state drives, floppy disks, zip disks, optical disks, tapes, memory cards, flash drives, and similar USB storage devices.
n.	Group MIS	Group Management Information System Department
o.	HGM	Head of Group MIS Department
p.	GSA	Group System Administrator (Infra) and System Administrator (Development)
q.	MIS Staff	Group MIS department technical support staff (technicians)
r.	Member(s)	INGRESS share holders

4.2 Conventions

The following is a list of conventions used in this document

a. **Shall** the use of the word 'shall' indicates a mandatory requirement.

b. **Should** the use of the word 'should' indicates a requirement for good practice, which should be implemented whenever possible.

c. **May** the use of the word 'may' indicates a desirable requirement.

5.0 INFORMATION SECURITY POLICY OVERVIEW

Everyone at INGRESS is responsible for familiarising themselves with and complying with all INGRESS's policies, procedures and standards dealing with information security.

5.1 Definition of Information Security

The National Information Assurance (IA) Glossary defines Information systems security as:

> *"The protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats."*

Information Security centres on the following three objectives for protecting information: Confidentiality, Integrity, and Availability. The policies in this document support these objectives.

5.2 Why Information Security?

INGRESS requires information security to protect information technology assets from information security threats. It is critical to protect the information system environment to maintain a competitive advantage in the marketplace, to ensure profitability, and to secure and maintain customer and partner trust and confidence.

Security threats originate at a wide variety of sources, including computer assisted fraud, industrial espionage, sabotage, vandalism and natural disasters. Computer viruses, unethical hacking and denial of service attacks are examples of threats encountered while operating over the Internet. These types of threats are becoming increasingly more common, more ambitious and more sophisticated, e.g. email SCAM, spoofing, web phishing etc.

5.3 Philosophy of Protection

INGRESS's philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

a. **Information Security is everyone's responsibility**. Maintaining an effective and efficient security posture for INGRESS require a proactive stance on information security issues from everyone. Information Security is not "somebody else's problem;" as an employee of INGRESS, all staff have the responsibility to adhere to the information security policies and procedures of INGRESS and to take issue with those who are not doing the same.

b. **Information Security permeates INGRESS organisation**. Security is not just focused on physical and technical "border control." Rather, INGRESS seeks to ensure reasonable and appropriate levels of information security awareness and protection throughout INGRESS organisation and infrastructure. There is no place in INGRESS business where security is not a consideration.

c. **Information Security is a business enabler**. A strong information security foundation, proactively enabled and maintained, becomes an effective market differentiator for INGRESS. Security has a direct impact on INGRESS viability within the marketplace, and must be treated as a valued commodity.

The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favour of another undermines the overall security posture of our organisation.

5.4 Critical Success Factors

The following factors are critical to the successful implementation of information security within INGRESS:

a. An information security approach that is consistent with INGRESS's culture;

b. Highly visible support from INGRESS's executive management;

c. Solid understanding of security requirements and risk management practices;

d. Effective communication of information security to all INGRESS managers, associates, partners, clients, vendors and developers;

e. Guidance on information security policy to all INGRESS managers, associates, partners, clients, vendors and developers;

f. Information security awareness and training;

g. Continual review and measurement of the effectiveness and efficiency of information security controls and mechanisms;

h. Timely adjustments to the information security posture by addressing deficiencies and by reflecting changes in INGRESS's business objectives as necessary;

i. Annual review of the information security policy to update policy as needed to reflect changes to business objectives or the risk environment.

5.5 Information Security Policy Structure

INGRESS's Information Security Policies are structured in such a way to give flexibility as required by the business objectives and needs while maintaining a 'level playing field' across INGRESS. Frequently, the weakest link is the link that breaks the security chain and causes a breach in security. Through consistent application of Information Security across INGRESS, any weak areas are compensated for and the organisation is stronger overall.

Information Security Policy follows this tiered structure:

a. **Information Security Mission Statement** – This is the overall management direction in regards to Information Security at INGRESS. It is broad in scope and sets the expectations for protecting INGRESS's information resources. It is contained in this document.

b. **Information Security Policy** – This is the collection of policies that implement the overall guidance of the Mission Statement. Policies are somewhat broad but topical in nature (centred on specific Information Security topics). INGRESS's Information Security Policies are organized in accordance with *ISO/IEC 27002:2013, Information Technology – Code of Practice for Information Security Management,* an international standard and is in compliance with other regulatory and compliance mandates where applicable. Policies apply equally to everyone within the company, regardless of location. The Information Security Policies are contained in this document.

c. **Information Security Standards and Processes** – These are collections of standards and processes that are to be used to implement the given policy they reference. Standards may dictate a type of technology to use, but may stop before naming a particular product (depending on the policy and standard subject). Processes will detail the steps to take to fulfil the goals of a particular policy. Standards and Processes will be published under separate titles

and may be regionalized to fit the conditions at different locations (i.e., there may be one set of standards for a particular policy in Malaysia, and a different set in Thailand and Indonesia). Standards and Process will clearly delineate where they apply.

d. **Information Security Specific Configurations and Procedures –** These are very specific details that support the implementation of the standards and processes given above. These will include specific products and configuration details, or step-by-step procedures to implement processes. These are very highly localised and will apply to the environment for which they were written (i.e., there may be a specific configuration for UNIX systems that is different from Microsoft Windows configurations. These will be published under separate titles where directed.

The hierarchy lends support as you progress up the tiers and becomes more detailed as you progress down the tiers. In this way, all actions taken have a basis in policy and directly support the policy or policies they are governed by. To illustrate this hierarchy, descriptions of the various levels are given below.

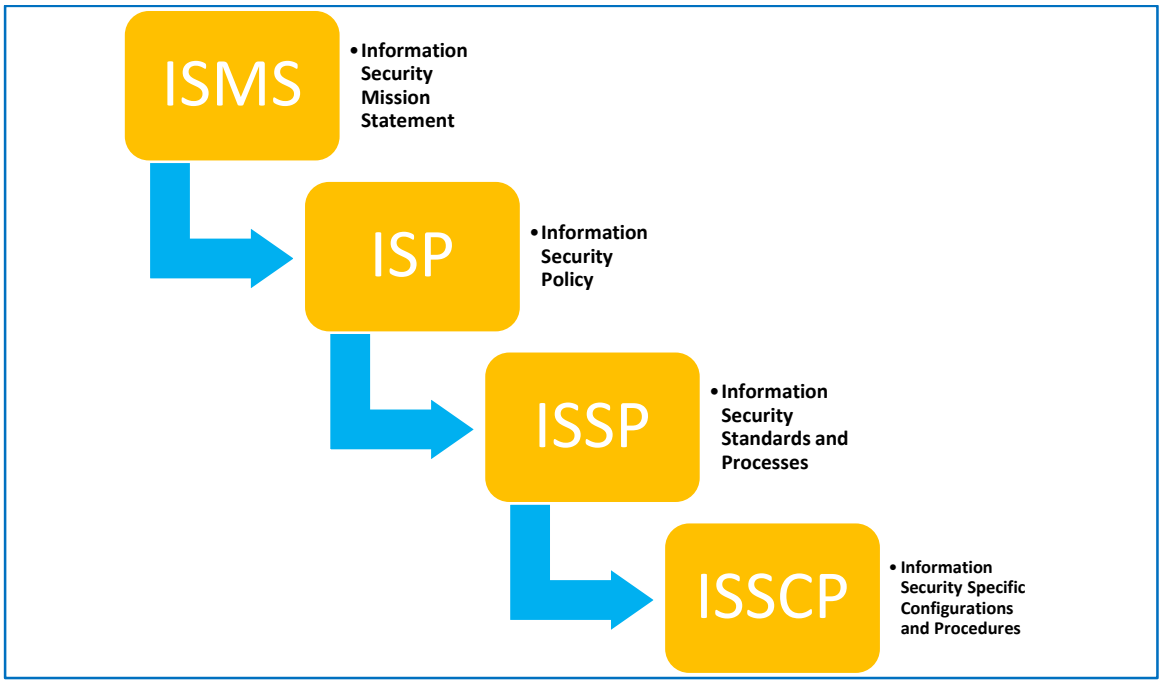

Figure 1: Information Security Policy Structure

6.0 INFORMATION SECURITY POLICIES

6.1 Information Security Policy Document

INGRESS Executive Management will provide direction for, approve, publish and communicate the merits of an Information Security Policy document. This Information Security Policy Document shall outline managements' approach to Information Security as well as providing the organisation with a strong indication of the management's commitment to Information Security within INGRESS.

The purpose of this policy is to communicate the direction of INGRESS's Information Security program by providing relevant, accessible and understandable definitions, statements and explanations.

The Information Security Policy Document shall:

a. Define information security as well as its scope and importance in INGRESS;

b. Include a statement of management's intent for information security;

c. Include a statement of management's goals and principles of information security;

d. Explain the organisation's security policies, standards and compliance requirements, including:

   i. Compliance with legislative and contractual requirements,

   ii. Security education and awareness commitment,

   iii. Consequences for information security violations.

   iv. Prevention and protection against viruses and other malicious software attacks,

   v. Commitment to well thought-out and effective business continuity management.

e. Outline specific responsibilities for information security management.

f. Outline policies and procedures for reporting security incidents.

The Information Security Policy Document shall serve as a reference document that will lead to additional more detailed information when necessary (for instance employee manuals etc.).

6.2 Review and Evaluation of Information Security Policy

The Head of Group MIS (HGM) shall be the owner of this Information Security Policy Document. The owner of the document shall be responsible for maintaining and reviewing the policy based upon a defined review process. The policy shall be reviewed at least annually and updated in response to any changes that would affect such as significant security incidents, new vulnerabilities, new regulations or changes to INGRESS's infrastructure.

The reviews shall include an assessment of the policy's effectiveness based upon:

a. The nature and number and impact of recorded security incidents;

b. Cost and impact of controls on business efficiency; and

c. Effects of changes to technology.

7.0 ORGANISATION OF INFORMATION SECURITY

7.1 Information Security Infrastructure

7.1.1 Allocation of Information Security Responsibilities

The purpose of this policy is to protect all of the information assets within the organisation by allocating specific responsibilities for all such assets.

a. The HGM is responsible for the overall application of the Information Security policies.

b. GSA is responsible for the implementation of the Information Security program in INGRESS.

c. Each individual site should have a dedicated MIS Staff who shall be responsible for the overall application of the Information Security Program and policies at that site.

d. Each information asset shall have an "owner", who may delegate responsibilities, but Group MIS remains ultimately responsible for the information asset(s).

The information asset owner should:

a. Identify and define all information security processes for their information asset(s);

b. Document all information security processes on their information assets; and

c. Clearly define and document all authorisation levels of their information assets

7.1.2 Authorisation Process for Information Processing Facilities

The purpose of this policy is to protect all of the information assets within INGRESS by authorising any new information processing facility for actual purpose and use, compatibility of hardware and software, and security of information assets in the facility.

The authorisation for new Information processing facilities requires that the HGM or GSA shall perform an assessment prior to authorising a new Information processing facility. This assessment should follow a standard format or checklist.

The results of the assessment will be incorporated to establish additional controls by INGRESS's GSA and the site MIS staff.

7.1.3 Specialist Information Security Advice

INGRESS may obtain the services of outsource security experts; as necessary, to protect the information assets within the organisation by co-coordinating in-house knowledge and experiences to ensure consistency, provide guidance in decision making, and assess the overall effectiveness of INGRESS's Information Security policy.

All use of outsource security experts shall be coordinated with the Head of Group MIS (HGM) before such experts are hired by INGRESS in any capacity.

7.1.4 Cooperation Between Organisations

All contact and cooperation with third parties on security matters will be coordinated through the Head of Group MIS (HGM) or a designated appointee by the HGM.

The purpose of this policy is to protect all of the information assets within INGRESS as soon as a security incident is detected by maintaining contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators.

The Group System Administrator (GSA) shall maintain a list of contacts with:

a. The law enforcement;
b. The regulatory bodies;
c. Information service providers;
d. Telecommunications operators.

7.2 Security of Third Party Access

7.2.1 Identification of Risks from Third Party Access

a. The Group System Administrator (GSA) will control authorisation for types of access to information processing facilities by third parties based upon the reasons for that access.
b. An assessment will be carried out before any third party access is granted and will consider the reasons for access as well as the necessary controls to be put in place.
c. Access of third parties to Information Processing facilities will be clearly spelled out in contracts; this access includes the scope of access to physical, logical and network assets.

7.2.2 Security Requirements in Third Party Contracts

The Group System Administrator (GSA) should control authorisation for types of access to information processing facilities and INGRESS information by third party contractors.

Any disclosure of confidential information to consultants, contractors, temporary employees, or any other third parties shall be preceded by the receipt of a signed INGRESS non-disclosure agreement (NDA) (see 8.1.1).

Access by third party contractors shall be specifically agreed upon and documented in contracts.

Arrangements involving third party access to organisational information processing facilities should be based on a formal contract containing, or referring to, all the information security requirements to ensure compliance with INGRESS's information security policies and standards. The contract should ensure that there is no misunderstanding between INGRESS and the third party. INGRESS should satisfy themselves as to the indemnity of their supplier.

The following terms should be considered for inclusion in the contract:

a. The general policy on information security;
b. Asset protection, including:
    i. Procedures to protect organisational information assets, including information data and software;
    ii. Procedures to determine whether any compromise of the information assets, *i.e. loss or modification of information data, has occurred*;
    iii. Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract;
c. Information Confidentiality, Integrity and availability;
d. Restrictions on copying and disclosing information;
e. A specific description of each service to be made available;
f. The target acceptable level of service and unacceptable levels of service;
g. Provisions for the transfer of staff where appropriate;

h. The respective liabilities of the parties to the agreement;

i. Responsibilities with respect to legal matters, i.e. data protection legislation, especially taking into account different national legal systems. If the contract involves cooperation with organisations in other countries *(see also 14.1)*

j. Intellectual property rights (IPR's) and copyright assignment (see 14.1.2) and protection of any collaborative work. (See also 8.1.1)

Information access control agreements, shall covering:

a. Permitted information access methods, and the control and use of unique identifiers such as user ID's and passwords;

b. An authorisation process for user access and privileges;

c. A requirement to maintain a list of individuals authorised to use the services being made available and what their rights and privileges are with regard to such use;

d. The definition of verifiable performance criteria, their monitoring and reporting;

e. The right to monitor and revoke user activity;

f. The right to audit contractual responsibilities or to have those audits carried out by a third party;

g. The establishment of an escalation process for problem resolution, contingency arrangements should also be considered where appropriate;

h. Responsibilities regarding hardware and software installation and maintenance;

i. A clear reporting structure and agreed reporting format;

j. A clear and specified process of change management;

k. Any required physical protection controls and mechanisms to ensure those controls are followed;

l. User and administrator training in methods, procedures and security;

m. Controls to ensure protection against malicious software (see 12.3);

n. Arrangements for reporting, notification and investigation of security incidents and security breaches;

o. Involvement of the third party with subcontractors.

These security requirements must address the confidentiality of INGRESS's data and the third party's relationships with any INGRESS competitor. This is especially important when dealing with engineering partners who work with various companies in the same space as INGRESS.

7.3 Information Security Outsourcing

7.3.1 Information Security Requirements in Outsourcing Contracts

The information security requirements of an organisation outsourcing the management and control of all or some of its information systems, networks and/or desktop environments should be addressed in a contract agreed between the parties.

The contract should address:

a. How the legal requirements are to be met, i.e. information data protection legislation;

b. What arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their information security responsibilities;

c. How the integrity and confidentiality of INGRESS's business information assets are to be maintained and tested;

d. What physical and logical controls will be used to restrict and limit the access to INGRESS's sensitive business information to the authorised users;

e. How the availability of services is to be maintained in the event of a disaster;

f. What levels of physical security are to be provided for outsourced equipment;

g. The right of audit.

The terms given in clause *7.2.2* should also be considered as part of this contract. The contract should allow the information security requirements and procedures to be expanded and to be agreed between the two parties.

8.0 HUMAN RESOURCE SECURITY

8.1 Security in Job Definition and Resourcing

8.1.1 Confidentiality Agreements

INGRESS expects that information disclosed to employees should be treated with the appropriate level of confidentiality. Except as required by law, information concerning INGRESS business is not to be discussed with competitors, outsiders, or the media. Employees are prohibited from forwarding e-mails containing confidential information on INGRESS business to anyone outside of INGRESS or otherwise transmitting INGRESS-confidential information outside of INGRESS, whether over the Internet or otherwise. Failure to honour this confidentiality requirement may result in disciplinary action, up to and including, termination of employment.

In the course of employee's work, they may have access to INGRESS's confidential and/or proprietary information, including information concerning staff (i.e. IC numbers) and suppliers, as well as fellow employees. It is imperative that no employees disclose such information in any inappropriate ways, and that such information be used only in the performance of regular job duties.

INGRESS requires confidentiality or non-disclosure agreements from all employees and third party staff not otherwise covered by third party contracts before access to sensitive information will be allowed.

This policy requires that staff sign a confidentiality or non-disclosure agreements (unless otherwise contractually bound) prior to being granted access to any sensitive information or systems.

Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organisation.

8.1.2 Terms and Conditions of Employment

INGRESS shall state the employee's roles and responsibilities for information security in the terms and conditions of employment.

The purpose of this policy is make clear to all employees their responsibilities for maintaining and promoting information security within the organisation during and subsequent to their employments as well as the sanctions for not doing so.

Group MIS will provide each new employee with the employee's responsibilities for Information Security in induction course (conduct by The Human Resource Department). This induction will contain information on Information Security policies, acceptable use, and ethics (direct information or instructions to obtain and read referenced policies).

Disciplinary measures are covered in clause 8.3.4 of this policy.

8.2 User Training

8.2.1 Information Security Education and Training

All employees will be appropriately trained on the INGRESS's Information Security policies and kept up-to-date on any additions or changes to the policies. Training is mandatory prior to receiving access to information system or information services.

Group MIS along with the Human Resources department is responsible for initial training and education on the INGRESS's security policies during the employee orientation process. Employees should have recurring annual refresher training on current threats, as well as material changes to policy. This training may be conducted by annual refresher seminars or continual reminders (such as e-mail)

When employees sign acknowledgements for complying with policy, these acknowledgements should include acknowledgement of initial training.

The HGM or representative will be responsible for the on-going policy education and training policy.

8.3 Responding to Security Incidents and Malfunctions

8.3.1 Reporting Security Incidents

Group MIS will educate employees on, and establish formal reporting and feedback procedures and incidence response procedures for all information security incidents. In this way, INGRESS will react to all information security incidents immediately and providing all employees with the necessary information to assist.

All suspected policy violations, system intrusions, virus infestations and other conditions that might jeopardize INGRESS information or INGRESS information systems shall be immediately reported to the GSA.

If an employee learns that INGRESS confidential information has been lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the employee shall immediately notify the "owner" of the information, MIS Staff or GSA.

Incidents may be used in on-going security awareness training to illustrate policy or procedures (see 8.2.1).

Incidents should be reviewed for the purposes of learning how they can be avoided in the future.

8.3.2 Reporting Information Security Weaknesses

INGRESS requires all users to immediately report suspected information security weaknesses in, or threats to, systems or services to MIS Staff or GSA's. These weaknesses should only be reported if actually discovered by the user, as the GSA will maintain a watch for vendor and notifications of new vulnerabilities (see 7.1.4).

Only users authorised by the GSA may test systems for suspected security weaknesses. Any unauthorised testing by users shall be considered misuse of the system and be subject to disciplinary measures.

8.3.3 Learning from Incidents

The purpose of this policy is to allow INGRESS to enhance INGRESS's information security policy to limit such occurrences in the future.

Incidents and malfunctions will be reviewed during the security review process (see 6.2). Analysis of incidents and malfunctions will be done to determine new controls that can be established to prevent future incidents.

8.3.4 Disciplinary Process

Disciplinary processes shall be documented by Human Resources and given to all employees and applicable third parties. Discipline for violating security policy or causing a security breach will be as appropriate, up to and including termination or possible criminal/civil charges.

If an employee is suspected of a breach of security, management shall be informed and the GSA, together with the HOD of the person suspected, shall begin the investigation.

9.0 ASSET MANAGEMENT

The purpose of this policy is to determine the protective controls associated with each INGRESS information asset and to provide a foundation for all employees (and contractors, third parties, etc. who deal with INGRESS information assets) to understand the security and handling of such assets.

INGRESS's information asset classification system (to refer "Information Asset Management & Classification Policy") has been designed to support access to information based on the need to know so that information will be protected from unauthorised disclosure, use, modification, and deletion. Consistent use of this information asset classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this information asset classification system, INGRESS unduly risks loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Applicable Information: This policy shall applicable to all information asset in INGRESS's possession, including electronic data, printed reports, backup media, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, all employees are expected to apply and extend these concepts to fit the needs of day-to-day operations.

9.1 Accountability for Information Assets

The purpose of this policy is to outline the methodology for identifying, classifying, and documenting information assets in order to provide protection that is commensurate with the value and importance of each asset. All users are expected to be familiar with and comply with this policy.

In order to maintain accountability for assets, Group MIS will compile a list of all its information assets, and establish the relative value and importance of each asset.

This policy requires that all information systems be identified and documented with a program in place to manage information assets company-wide. The following will be included in the program:

a. All information assets associated with each information system shall be identified and documented with their classification, owner, and location;

b. All information assets shall have an owner (see 7.1.1) and that owner shall be documented;

c. All information assets shall be classified (see 9.2) based upon their value and importance to the organisation;

d. Classification of information security assets will reflect their information security protection levels (see 9.2) and their handling (see 9.2.1.3);

e. Information Assets should be categorised into logical categories such as information assets, software assets, physical assets and service assets;

9.2 Information Classification

9.2.1 Classification Guidelines

Information Asset classification is the process of assigning value to information data in order to organize it according to its sensitivity to loss or disclosure. All information assets shall be classified, using a company-wide asset classification system. All data, regardless of its classification, will be protected from unauthorised alteration; this policy provides guidance on the proper handling of data.

The information classification system will allow that classifications of information assets may change over time (see 10.1).

9.2.1.1 Classifying Information

This policy requires that all information assets be classified and labelled in a manner that allows the asset to be readily identified to determine handling and protection level for that asset.

Care will be taken when interpreting the information classification systems from other organisations as their information classification systems may have different parameters. Information assets shall be assigned a sensitivity classification by the asset information owner or their nominees, in accordance with the following classification definitions:

a. Confidential: Sensitive information requiring the highest degree of protection. Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires the information custodian's approval and, in the case of third parties, a signed confidentiality agreement. If this information were to be compromised, there could be serious negative financial, legal, or public image impacts to INGRESS or INGRESS's members. Examples include member share information, employee performance reviews, product research data, etc.

b. Internal: Information that is related to INGRESS business operations, but not available for public consumption. This information shall only be disclosed to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm to INGRESS, and access is provided freely to all employees. Examples include policies and standards, operational procedures, etc.

c. Public: Information that requires no special protection or rules of use. This information is suitable for public dissemination. Examples include press releases, marketing brochures, etc.

HGM is responsible for maintaining the policy and ensuring the infrastructure exists to support this policy.

9.2.1.2 Handling and Protection Rules

Each information asset classification shall have handling and protection rules. These rules must cover any media the information assets may reside in at any time (see 9.2.1.3).

All computer-resident confidential information shall be protected via access controls to ensure that it is not improperly disclosed, modified, deleted or otherwise rendered unavailable.

Employees are prohibited from recording confidential information with tape recorders, digital/analogue recording devices, camera equipment (of any kind) etc., without the

consent of the information asset "owner". Unless it has specifically been designated as "Public". All INGRESS internal information should be assumed to be confidential and should be protected from disclosure to unauthorised third parties.

No confidential information of INGRESS or of any associate third party shall be disclosed to the public or any unauthorised third party without the prior approval from the "owner" or GSA.

Access to every office, computer room, server room, and work area containing confidential information shall be restricted, and employees shall take all reasonable steps to protect confidential information under their control from inadvertent disclosure.

Handling and protection rules must include all parts of an asset's life-cycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

9.2.1.3 Information Labelling and Handling

It is important that an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by INGRESS. These procedures should cover information assets in physical and electronic formats. For each information classification, handling procedures should be defined to cover the following types of information processing activity;

a. Copying;
b. Storage;
c. Transmission by post, fax, and electronic mail;
d. Destruction;

System outputs containing confidential information shall carry an appropriate information classification label (in the output).

The labelling should reflect the information classification according to the rules established in clause 9.2.1. Items for consideration include printed reports, captured screen displays, recorded media (tapes, disks, CD's, cassettes), and electronic messages and file transfers.

Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used.

9.3 Information Retention

Information shall not be retained any longer than the business requires it to be retained. This reduces the window of time that data can potentially be available for misuse. Controls should be implemented to delete data that exceeds required retention time.

10.0 ACCESS CONTROL

10.1 Business Requirement for Access Control

10.1.1 Access Controls and Need to Know

Group MIS should define and document access control rights and rules for each user or group of users.

a. Service providers and vendors shall be given clear statements of the business requirements met by these access controls:

   i. Access to information and information services shall only be given on the basis of business and security requirements.

   ii. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information and without compromise to associated information or raw data.

b. Data owners shall review access control rights for users and groups of users on a bi-annual basis to ensure that all access rights are authorised and remain appropriate, and to ensure no unauthorised privileges have been gained.

   i. Access shall be given that is consistent with security levels and classifications, consistent with legislation and contractual obligations for confidentiality.

   ii. Access to standard common groups of users should be given standard access profiles.

   iii. Access rights in a networked environment should recognize all connection types available.

   iv. All users and groups of users shall receive a clear statement as to the policy and as to the requirements met by these access controls.

c. The owner of confidential information shall decide who will be permitted to gain access to that information, and shall specify the uses for that information.

d. Administrator access to production systems will be limited to only those with a justified business requirement for such access.

e. Developers and other application personnel shall not have access to the underlying operating system on production systems, except in emergencies and then with access only granted for a limited time.

f. GSA should not have access to the applications if possible.

10.1.2 Types of Access Controls

Group MIS should established clear access control rules that distinguish between optional, express, discretionary, automatic and those that require approval.

a. Access rules should specifically differentiate between those rules that are optional or conditional and those that are always to be enforced.

b. Access rules should be declarative statements such as “access is forbidden unless specifically permitted” instead of “access is generally permitted unless forbidden”

c. Access rules should differentiate between those rules that require approval and those that do not.

d. Access rules should consider changes in classifications that are automatic (see 9.2) and those classification changes that must be initiated by an administrator.

e. Access rules for each system should be developed in according with this policy commensurate with the information's sensitivity (see 9.2).

10.2 User Access Management

10.2.1 User Registration

A formal user registration and deregistration process should be used for gaining access to multi-user systems. This process must protect and maintain the security of access to INGRESS's information resources through the complete life cycle of the user.

a. Access to INGRESS confidential information shall be provided only after the authorisation of the information owner has been obtained.

b. Contractors and third party contracts should contain the rights of access and should contain sanctions if unauthorised attempts at access are made (see 8.1.2 and 8.3.4)

c. Service providers and vendors shall be made aware of the policy which not to provide access to users until specific authorisation has been given.

d. Each person accessing a multi-user based information system shall utilise a unique assigned User ID and a private password. User IDs shall not be shared among two or more users.

e. System owners and/or GSA shall grant access rights. Formal records of all access rights for each information system shall be maintained.

f. Access rights shall immediately be removed or modified when a user leaves the organisation, terminated, retired, or transferred.

Group MIS will periodically check for redundant IDs and ensuring that redundant IDs are not issued in excess of that required (i.e., administrators may have a privileged and a non-privileged account on the same system, but an average user should not have two different non-privileged accounts on the same system without a valid business reason).

10.2.2 Privilege Management

User rights shall be granted using the Principle of Least Privilege (POLP), based on business need and security requirements.

All privileges shall be granted only with formal authorisation. This authorisation shall be accomplished along with User ID authorisation. All privileges that are granted will be documented. No privileges shall be granted until authorisation is complete.

Elevated Privileges (EP) (Administrator or root, etc.) should be assigned to a different user ID than that used for normal business use. Administrators should only use their elevated privilege accounts when conducting activities that actually require them. Elevated privileges must only be assigned to dedicated systems administrators and not normal users.

10.2.3 User Password Management

a. A user's account and password is the primary means of verifying a user's identity. The allocation of passwords will be a formal management process.

b. Users will sign a statement in their terms and conditions of employment (see 8.1.2) that they will keep their personal or group passwords confidential. This may be done as part of the overall acceptance of policies.

c. Users will be responsible for the secure of their passwords.

d. Users will be granted initial temporary passwords and will be forced to change them immediately. Temporary passwords will only be granted with positive identification of the user.

10.2.4 Review of User Access Rights

a. Users' access rights shall be reviewed at regular intervals. Head of department will review their staff's rights to ensure they are consistent with their present job function.

b. Group MIS will review user rights to ensure that elevated privileges have not been granted out without authorisation, and that accounts that have not been used recently or belong to terminated employees are deactivated or purged.

c. User access rights shall be reviewed at least every 6 months. Privileged access rights shall be reviewed every 3 months to ensure that all are authorised and remain appropriate and that no unauthorised privileges have been gained.

10.3 User Responsibilities

10.3.1 Password Use

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of INGRESS's entire corporate network. As such, all INGRESS employees (including contractors and vendors with access to INGRESS systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any INGRESS facility, has access to the INGRESS network, or stores any non-public INGRESS information.

10.3.1.1 User Password Rules

a. All users shall keep their passwords confidential and store them securely (i.e. not on the computer and not on paper unless they can be protected).

b. Users should be made aware of good security practices and the requirement to use good security practices with their passwords.

c. All passwords shall be treated as confidential INGRESS information. They should not be shared with anyone.

d. Password requirements:

i. If an account or password is suspected to have been compromised, report the incident to MIS Staff and change the passwords;

ii. Regular passwords shall be changed at least every 3 months (90 days).

iii. Privileged passwords shall be changed every 90 days.

iv. Shared privilege passwords (i.e. for “root”, “administrator”, etc.) should be changed every 90 days or whenever someone with administrator-level access leaves the firm.

v. Passwords cannot be re-used for a minimum of 12 months or 4 passwords.

vi. Temporary passwords will be changed at first log-on.

vii. Systems shall be configured to lock user accounts in the event of 3 consecutive unsuccessful login attempts.

viii. System Administrators may reset locked accounts; otherwise the minimum account lockout duration shall be 24 hours.

ix. Passwords shall not be stored on a computer or used in a macro for sign-on.

x. User shall not use the "Remember Password" feature of any applications.

xi. Passwords should not be appear in e-mail messages or other forms of electronic communication.

xii. Passwords should not be written down or stored unencrypted on ANY computer (including Smartphone)

10.3.1.2 System Password Rules

a. System accounts (i.e., non-interactive accounts for specific applications or systems) must use passwords that meet or exceed the password composition requirements (see 10.3.1.3).

b. System-level passwords must be changed at least once every 90 days.

10.3.1.3 Password Composition

All user-level and system-level passwords must conform to the requirement described below.

a. Passwords shall be at least 8 non-sequential characters long.

b. Passwords shall be composed of alpha-numeric characters.

c. Passwords shall contain all of the 4 characteristics below:

i. alphabet character (a, b, c…z)

ii. upper case letter (A, B, C…Z)

iii. number (0, 1, 2, 3…9)

iv. special character (@, $, !...etc.)

10.3.2 Unattended User Equipment

Users shall protect INGRESS’s information resources from unauthorised access by protecting unattended equipment:

a. Users will terminate active sessions when finished (or unattended) or secure by appropriate locking functions.
b. Users should log-off of multi-user systems when finished.
c. A password-protected screen saver should be automatically invoked after 15 minutes of inactivity.

10.4 Network Access Control

10.4.1 Policy on Use of Network Services

Users shall only have access when there is a specific business requirement and the access has been specifically authorised.

a. Users should be granted specific access through networks that they are permitted to access.
b. Users shall not access networks that they are not given specific authorisation to access.
c. Group MIS shall provide users with the rules, policies and procedures for accessing network connections and network services.
d. Third parties that must deploy non-INGRESS controlled systems must be specifically approved by the HGM and must meet the security of third party access (see 7.2.2).

10.4.2 User Authentication for External Connections

INGRESS employee remote users shall be required an approval from the data owner and properly authenticated before they are permitted to access internal information resources.

a. Users should be given remote access only with limited time when their job function requires it.
b. Any non-employee who receives approval for remote access must be to access to specific systems only.
c. All procedures and controls shall be thoroughly tested prior to use.

10.4.3 Segregation in Networks

10.4.3.1 External Segregation

GSA should segregate groups of information services, users and information systems when interconnecting networks to partners or other third parties.

a. An assessment should be performed to determine the necessary controls prior to allowing access of INGRESS networks by new partners or third parties, and the GSA must approve of any such connections.
b. Network segregation controls will be selected on the basis of the assessment; cost and the impact of incorporating suitable routing and gateway technology (see 9.4.7 and 9.4.8).
c. There shall be no direct connection between the INGRESS corporate (internal) network and any third party. See also 7.2.

10.4.3.2 Internal Segregation

Based on site assessments (see 11.1.1), internal segregation of sites or networks within sites may be warranted.

Development and testing networks/systems must be segregated from the rest of the internal network (either completely or through a firewall/proxy arrangement) to prevent malfunctions in software from impacting the rest of the network. In addition, certain locations (such as locations where there is civil unrest or rampant crime) must be adequately segregated from the rest of the network to ensure the security of corporate information assets.

Confidential information should be consolidated and isolated on dedicated access servers, active storage and inactive storage (such as tape media) whenever possible.

10.4.3.3 Segregation of Development and Production Environments

INGRESS will separate development and production environments to prevent unfinished or malfunctioning software from affecting the business network. Only approved systems will be connected to production environments, and only after the systems have fulfilled acceptance criteria (see 12.2.2)

10.4.4 Network Connection Control

Highly sensitive systems shall have network access controls (i.e., firewalls or Access Control Lists) in place to prevent unauthorised connections from inside, or outside INGRESS. This is in addition to any application or system access controls. Restrictions will be consistent with this policy.

Network controls shall be configured to allow only network traffic required by the business to enter or leave the INGRESS network. The GSA shall work with Business Unit management to determine those business requirements. These controls shall include:

a. Ingress and egress filtering on border devices

b. Firewall/Access Control List configuration that is host and port specific.

10.4.5 Wireless Network Policy for INGRESS Facilities

This policy shall identify measures to access to INGRESS corporate networks via wireless communication mechanisms.

This policy covers all wireless data communication devices (i.e., personal computers, cellular phones, Smartphones, etc.) connected to any of INGRESS internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to INGRESS corporate networks do not fall under the purview of this policy.

10.5 Operating System Access Control

10.5.1 User Identification and Authentication

All users shall be identified and authenticated with the minimum of a unique identification and a password before access to operating systems is granted. This will minimize the opportunity for unauthorised access to information resources at the operating system level by providing a means of user authentication.

If operating system access is necessary, such access will abide by the following rules:

a. All users shall have a unique user account (see 10.2.1)

b. All users shall have a unique password (see 10.2.3)

c. Users' passwords will give no indication to their privilege level

d. Passwords (see 10.3.1 and 10.5.2)

10.5.2 Password Program

All passwords for systems and applications must be individual, effective, and of sufficient quality to deter compromise. Systems and applications must be configured to programmatically enforce these rules if available. In the absence of programmatic enforcement, the user will be responsible for enforcing these rules themselves. See 10.3.1 for more information on passwords.

10.5.2.1 System Password Rules

a. Default passwords will be changed as soon as a new application is installed.

b. Systems must automatically expire passwords on the anniversary of the creation of the password. Expiration may lead to disabling of the account or forcing a password change (depending on the software implementation).

c. Application developers must ensure their programs contain the following security precautions. Applications:

i. should require confirmation during selection to avoid input errors

ii. should support authentication of individual users, not groups

iii. should not store passwords in clear text or in any easily reversible form

iv. should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password

v. should keep password files separate from application system data

10.5.3 User Account Review/Audit

All user accounts shall be reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist. User/group roles and access rights shall be reviewed on a regular basis to ensure that no user or group has excessive privileges.

10.5.4 Use of System Utilities

Access to system utilities for non-administrators should be restricted to minimize the opportunity for unauthorised access to or modification to information resources.

All unnecessary system utilities shall be removed from server systems. Unnecessary system utilities should be removed from desktop/laptop systems as appropriate.

10.6 Application Access Control

10.6.1 Information Access Restriction

To safeguard applications, INGRESS will restrict business application system access information on a need-to-know basis (see 9.1):

a. Menus and documentation shall be edited so the users only view data or menus that they are authorised to view.

b. Users' rights shall be based on a Least-Privileged basis, so that they limited to only those functions to which they are authorised (i.e. read, write, delete, and execute).

c. User's rights shall be reviewed on a periodic basis to ensure that no user or group has excessive privileges.
d. Outputs available to users are limited to those to which they are authorised.
e. Sensitive outputs shall be controlled and limited to specific terminals and/or printers.
f. Sensitive outputs shall be controlled and limited to specific users who have a valid business need.
g. Periodic reviews will be performed to ensure that outputs of sensitive information are required by the business.

10.7 Monitoring System Access and Use

10.7.1 Event Logging

a. INGRESS will log all security-relevant events or exceptions.
b. MIS Staff will be responsible for maintaining event logs.
c. Event logs will be retained for at least one year with at least 3 months of on-line retention.
d. GSA will monitor event logs at periodic intervals, not to exceed weekly. Automated log analysis and alerting will suffice for this provision.
e. Event logs will contain:
    i. User IDs used in logons
    ii. Dates and times for logon and logoff for each user
    iii. Terminal identity (system name or network address)
    iv. Successful and rejected access attempts
    v. Successful or rejected data access attempts
    vi. Use of elevated privileges through 'su' or 'run as'

10.7.2 Monitoring System Use

INGRESS will monitor the use of information processing facilities to detect unauthorised activities and ensure that users are only performing the functions and gaining access to information to which they are authorised.

Each facility shall perform an assessment to determine the level of monitoring required.

10.7.2.1 Monitored Items

Areas eligible for monitoring include:

a. Authorised access:
    i. User IDs
    ii. Date and time of key events
    iii. Types of events
    iv. Files accessed
    v. Programs and utilities used
b. Privileged operations:
    i. Use of supervisor accounts
    ii. Use of other privileged accounts (i.e. administrator)
    iii. System start-up and stop

iv. Device attachment and removal

c. Unauthorised attempts:

i. Failed attempts for access

ii. Access policy violations and notifications for network gateways and firewalls

iii. Alerts from proprietary intrusion detection systems

d. System alerts or failures:

i. Console alerts or messages

ii. System log exceptions

iii. Network management alarms

iv. All access to Member data, including root/administration access

Monitoring results shall be retained in accordance with retention schedules for potential evidence.

10.7.2.2 Review of Monitored Information

MIS Staff and the GSA should regularly review the results of the monitoring of information processing facilities to detect deviations from INGRESS access control policy and to improve and discipline those that deviate.

The factors that determine the frequency of review include:

a. Value, criticality or sensitivity of the information or application involved;

b. Past experience of infiltration or misuse; and

c. Extent of interconnections.

d. Those who violate policies shall be disciplined (see 8.3.4).

e. Incidents shall be reviewed and controls put in place to stop future occurrences (see 8.3.3).

10.7.2.3 Protection of Monitored Information

a. Event and security logs shall be protected in order to assure their accuracy and to protect them against tampering or misuse.

b. All original logs shall be kept unaltered.

c. Extracted log events shall be kept separately from the original logs.

d. Controls shall be put in place that prevent and monitor:

i. attempts to de-activate logs

ii. attempts to alter message types that are recorded

iii. attempts to edit or delete log files

iv. the log file becoming exhausted and either overwriting itself or failing to record events

v. The System owners shall be responsible for the reviewing of their system logs.

10.7.3 Clock Synchronization

GSA should use a common method to ensure that all system clocks are synchronized. This will ensure the accuracy of the audit logs, and protect the integrity and credibility of any logs that might need to be used as future evidence.

10.7.4 E-Mail and Internet Access Monitoring

INGRESS's e-mail and Internet access systems are to be used primarily for INGRESS business. INGRESS reserves the right to access e-mail systems at any time with or without advance notice or consent of the employee. Such access may occur before, during or after working hours by any Group MIS staff or personnel designated by INGRESS.

Employees should not have an expectation of privacy in their e-mail messages, or in computers or computer storage devices. INGRESS also reserves the right to monitor all Internet access. While Group MIS recognizes that accidental access to undesirable sites is unavoidable, prolonged or repeated access to undesirable sites will be construed as intentional violation of INGRESS's policy and may result in disciplinary action up to and including termination.

All Internet data that is composed, transmitted or received via INGRESS's computer communications systems is considered to be part of INGRESS's official records and, as such, may be subject to disclosure to third parties. Employees should always ensure that the business information contained in Internet transmissions is accurate, appropriate, ethical, and lawful.

10.8 Mobile Computing and Teleworking

10.8.1 Mobile Computing

INGRESS institutes the following policies to ensure that business information is not compromised by use of such devices as tablet, laptops, smartphone, and mobile telephones in an unprotected environment and to provide users with controls for and awareness of the potential risks.

An assessment will be performed on the potential threats associated with the various forms of mobile computing for new devices (other than those listed above) that become available.

The assessment will consider the following issues:

a. Physical protection of the device (i.e. locking device)
b. Access control (see 10.1),
c. Back-up schedules, procedures and media protection (see 12.4),
d. Protection from viruses and malicious software (see 12.3),
e. Network connections (see 10.4),
f. Use of networking facilities in public places.

Users of mobile computing devices will be required to sign a statement of their understanding and compliance.

10.8.1.1 Physical Protection of Mobile Devices

Users must reasonably ensure mobile devices are physically secure at all times if they contain INGRESS sensitive data. Examples of physically securing devices include:

a. Mobile devices should never be left visible in a car, and should never be left in the trunk or other unsecure storage location overnight;
b. Mobile devices should always be carried on-board aircraft and not put in checked luggage;
c. Mobile devices should not be left at tables in public places (i.e. restaurants) if they will be out of sight.

10.8.1.2 Access Control Requirements

If a mobile device contains other than public INGRESS data, it must have some form of access control to access this information. If access to the device is not controllable, access to the data must be controlled.

10.8.1.3 Information Backup

Users are strongly encouraged to back up their INGRESS data stored on mobile devices. Backup may be done when connected to the INGRESS network (file shares and other backup facilities), or may be backed up to removable media. If backed up to removable media, this media must be physically protected or the data must be encrypted and was not kept in the same place with the mobile device.

10.8.1.4 Protection from Viruses/Malicious Software

If capable, mobile devices must run anti-virus software with current updates/definitions. All laptops must use Group MIS approved anti-virus software.

10.8.1.5 Connecting to the INGRESS Network

Users shall only connect personal mobile devices that have been authorised by the GSA to the INGRESS network. These devices shall have current anti-virus software running and the user must be reasonably sure no other malicious software is operating on the laptop.

Users shall never connect to an outside network through any form of network interface (broadband modem, wireless, second Ethernet card, etc.) while simultaneously connected to the internal INGRESS network through their primary network connection. If use of a secondary connection is necessary, the user must first disconnect from the INGRESS network before connecting to the outside network.

MIS Staff shall have the right to check users approved personal mobile devices before connecting to the INGRESS network if they have reason to believe they may have come into contact with any malicious software, whether detected by anti-virus or not.

10.8.1.6 Connecting to the Internal INGRESS Network from Public Places

Remote connections to the INGRESS network may be made by mobile devices at public places under the following provisions. Public places are defined as any place outside an INGRESS facility and include, but are not limited to hotels, hot spots at food or drink establishments, airports or train stations, employee's or other people's homes, government or partner facilities.

Users should use an approved personal firewall, and have it running and actively filtering traffic, when connecting to INGRESS networks from public places. Users must also have current and active anti-virus software running before connecting. Remote connections will be made through dedicated VPN tunnels to safeguard the connection traffic. Connections from home networks may use a gateway firewall (such as a Linksys router with firewall or other similar SOHO firewall) in place of the personal firewall, but one or the other must be operational and actively filtering traffic. Note that if the SOHO firewall includes wireless functionality, the personal firewall must also be used (see below).

10.8.1.7 Wireless Connections (Any)

INGRESS users should use a personal firewall and anti-virus software (as discussed above) whenever connected to a wireless network, regardless of whether or not they will connect

to the INGRESS networks. In addition, the use of WPA or equivalent privacy measures is encouraged where available.

Mobile device users should not enable ad hoc networking, or operate any other access point functionality on their wireless adapters while connected to the INGRESS network through another connection (Ethernet, broadband modem, etc.).

10.8.2 Telecommuting and Remote Access

The purpose of this policy is to ensure that the organisation's information resources are not compromised by those that access them from premises that are not under the control of INGRESS by requiring authorisation, controls and monitoring the telecommuting. Also see 10.8.1 concerning mobile devices.

Users shall strictly control and protect INGRESS's information resources against the possible threats associated with telecommuting. These threats include theft of the remote computing devices and unauthorised access into INGRESS's computing facilities.

Revocation of remote access rights shall be immediate as soon as telecommuting ceases.

An annual assessment should be performed to review users who have remote access privileges to ensure that their job requires them to use remote access services.

10.8.2.1 Authorisation for Remote Access

All telecommuting (work that occurs from a fixed location that is outside of the organisation that requires connection to the INGRESS's information resources) shall be authorised by the GSA.

Authorisation Rules:

a. All telecommuting will be specifically authorised,
b. The access to sensitive information shall be specifically authorised,
c. The storage of sensitive information shall be specifically authorised,
d. The work performed by the telecommuting shall be specifically authorised,

Telecommuting Resources:

a. The telecommuting shall have adequate and secure communications equipment,
b. The teleworker shall be given access to hardware and support and maintenance services,

Communication requirements will be secure and in-line with those required by the information to be accessed classification (see 8.0).

10.8.2.2 Applicability of This Policy during Telecommuting

Users shall responsible for any security breaches that occur as a result of their negligence in securing their personal remote systems. By using their own equipment, users are accepting responsibility to protect the INGRESS information in accordance with policy. INGRESS reserves the right to audit and monitor any equipment used to process or store INGRESS information resources, regardless of ownership.

10.8.2.3 Remote Access Methods and Authentication of Connections

Users shall employ only INGRESS approved remote access methods when connecting to the INGRESS network.

This provision applies equally to the connection to the INGRESS network and connections to INGRESS information resources within the network. Only approved methods of system remote access will be allowed in accordance with information security guidance and standards. All use of non-approved access methods, or approved access methods not utilising Group MIS approved configurations and settings, will be subject to disciplinary procedures (see 8.3.4).

Access to the INGRESS Networks via remote access is to be controlled using strong authentication.

10.8.2.4 Remote Management of Systems

Where possible, remote connections should not allow logon via an elevated system account (i.e., root or administrator) directly. Administrators must log on with their user account and then change to the elevated privilege account. This will ensure accountability and logging of unique IDs instead of shared administrative accounts.

10.9 Acceptable Use of INGRESS Computer Systems

The purpose of this policy is to outline the acceptable use of computer equipment at INGRESS. This will help protect INGRESS's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use exposes INGRESS to risks including virus attacks, compromise of network systems and services, and legal issues. All users are expected to be familiar with and comply with this policy.

All INGRESS systems are to be used for business purposes in serving the interests of the company, and of INGRESS clients and members in the course of normal operations, although occasional use of INGRESS computer systems for personal use is acceptable.

Effective security is a team effort involving the participation and support of every INGRESS employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know this policy, and to conduct his/her activities accordingly.

This policy applies to employees, contractors, consultants, temporaries, and other workers at INGRESS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by INGRESS and personal equipment that is used to connect to INGRESS network.

10.9.1 General Use and Ownership

While INGRESS's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of INGRESS. Because of the need to protect INGRESS's network, management cannot guarantee the confidentiality of information stored on any network device belonging to INGRESS.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Group MIS are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, and if there is any uncertainty, employees should consult MIS Staff or GSA.

Employee shall exercise due diligence to protect sensitive or confidential data or material. For guidelines on information classification, see 9.2.

For security and network maintenance purposes, MIS Staff have the right to monitor equipment, systems and network traffic at any time.

10.9.2 Security and Proprietary Information

Employees shall take all necessary steps to prevent unauthorised access to this information:

a. Authorised users shall responsible for the security of their passwords and accounts. Users must keep their passwords secure and accounts should not be shared.
b. All desktops and laptops should be secured with a password-protected screensaver with the automatic activation feature set at least minimum 15 minutes, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
c. All applicable hosts used by the employee that are connected to the INGRESS network, whether owned by the employee or INGRESS, shall continually execute approved virus-scanning software with a current virus database.
d. Employees must use extreme caution when opening e-mail attachments received, especially from unknown senders, as these attachments may contain viruses, e-mail bombs, or Trojan horse code.

10.9.3 Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of INGRESS authorised to engage in any activity that is illegal under local, state, federal or international law while utilising INGRESS owned resources.

The lists below are by no means exhaustive, but provide a framework of strictly prohibited activities:

10.9.3.1 System, Network, and Internet Activities

a. Private use of the Internet may be permitted within reasonable limits, provided that the Web sites accessed are not unlawful or inappropriate to a well-controlled working environment (e.g. pornography, gambling or drug-related sites etc.).

b. The Internet must not be used to violate intellectual property rights of any party. Intellectual property includes copyrights, trademarks, patents, trade secrets, publicity and privacy rights. Employees are prohibited from interfering with or attempting to disable anti-piracy mechanisms or other standard technical measures used by copyright owners to protect or identify their work.

c. Accessing resources other than web sites on the Internet from INGRESS premises is reserved to the authorised users of the target systems, must be limited to legitimate purposes. Attacking in any way, as well as scanning, probing or penetrating, computer systems or networks on the Internet is strictly prohibited. All employees will be made aware that all Internet access may be screened, logged and monitored, in accordance with this policy (see 10.9.1).

d. INGRESS reserves the right to block access to Internet sites considered inappropriate. Deliberate attempts to access such sites will result in disciplinary action.

e. The download of electronic files from the Internet by employees is prohibited unless as a necessary part of their work and must be subject to virus checking on the local workstation.

f. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which INGRESS or the end user does not have an active license is strictly prohibited.

g. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

h. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

i. Employees shall not reveal/share account passwords to others or allow use of their accounts by others. This includes family and other household members.

j. Employees shall not use an INGRESS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

k. It is not permissible to make fraudulent offers of products, items, or services originating from any INGRESS account.

l. Employees shall not attempt to access data for which they have not been granted access, unless they have been granted permission to test security controls of a system or application (i.e. these duties are within the scope of regular duties).

m. It is prohibited to execute any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.

n. It is prohibited to circumvent user authentication or security of any host, network or account.

o. It is prohibited to provide unauthorised information about, or lists of, INGRESS business and INGRESS employees to parties outside INGRESS.

10.9.3.2 Email and Communications Activities

a. Personal, non-business use is permissible to the extent that it does not consume significant resources, and that it does not pre-empt any business activity.

b. The use of unapproved instant messaging systems (e. g. AOL Instant Messenger, ICQ) is not permitted.

c. Employees shall not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

d. It is prohibited to participate in any form of harassment via email, telephone or media, whether through language, frequency, or size of messages.

e. Unauthorised use, or forging, of email header information is prohibited.

f. Employees shall not use INGRESS email or computing resources to participate in the creation of or the forwarding of "chain letters", "Ponzi", or other "pyramid" schemes of any type.

10.9.4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11.0 PHYSICAL AND ENVIRONMENTAL SECURITY

11.1 Secure Areas

11.1.1 Physical Security Controls

Physical entry controls will be used to protect all secure areas. These controls should be designed to prevent unauthorised access, damage or interference to the business processes that take place within the area. Physical security controls apply to any INGRESS owned or controlled facility, including temporary locations.

11.1.1.1 Site Assessment

An assessment of secure areas to determine the type and strength of the physical entry control that is appropriate and prudent. The security controls for an area should be commensurate with the value and classification of the information resources contained therein (see 9.2). This assessment must also take into account the physical surroundings of the site (see 11.1.2). Finally, physical security requirements should include items such as fire suppression, plumbing, and electrical wiring as these may not always be mandated by local authorities.

Site assessments must be conducted for any sites where INGRESS will be sharing facilities with any outside organisation. This may be sharing a building (where physical access is common to all, but network access is specific to each organisation) or where INGRESS is sharing a suite (where physical and network access is common to all) with others. Specific security requirements must be determined for these situations, based on the arrangements.

When sites are deficient in physical security controls (such as leased sites where the owner will not allow modification to the structure, or shared sites with business partners), additional network security controls are warranted to protect the rest of the corporate network. In addition, the levels of sensitivity of information that can be processed or stored there may be restricted.

11.1.1.2 Restricted Access to Sites

Controls for restrict access to facilities will be determined on a case-by-case basis. These controls will ensure that unauthorised persons do not have easy physical access to the facilities, and such access is detected and the appropriate personnel notified if a breach occurs. GSA will publish procedure for access controls and other physical security measurements commensurate with the classification levels of data present and the information protection requirements (see 9.2.1).

Some common controls is as below;

a. Access to sensitive information and information processing facilities will be restricted to authorised personnel only.

b. Authentication controls will be used to authorise and validate entry.

c. A log of all that enter will be maintained by the site MIS Staff as appropriate for the sensitivity of the information resources therein (see 9.2.1).

d. Physical barriers (i.e., doors) must be of sufficient strength and construction to deter entry, based on the results of the assessment.

Access rights will be given on a least-privilege basis, and will be as granular as necessary to appropriately protect various classifications of information or facilities. Access rights to secure areas will be reviewed by the GSA periodically and updated where necessary.

11.1.1.3 Visitor Procedures

All visitors to secured areas shall be supervised and only allowed in for authorised purposes. A visitors' log shall be in place at all secure areas that records date and time of entry and exist times. All visitors should be given both security instructions and emergency procedures (if applicable).

MIS Staff shall challenge unfamiliar people who are unescorted or not showing visible identification.

Contractors, service vendors, suppliers, material men, etc., should be advised of the secured area rules and regulations concerning their proper conduct within INGRESS's property.

11.1.1.4 Third Party Physical Security at INGRESS Facilities

Special situations may arise where third parties will have personnel and devices at INGRESS facilities on a full time basis. These third parties must only be allowed full time access if they serve to augment the core capability or flow of INGRESS's business. Special care should be taken to limit access of third party personnel to only their work areas as much as possible.

Controls for the placement of third party devices on INGRESS networks are covered in clause 12.2.2.

11.1.1.5 Control of Physical Security Controls

Access to the mechanisms that control physical access to secure sites must be done on the least-privilege basis. This includes access to badge enabling systems, door lock keys, or any other physical access control systems. Master badges or keys must be restricted to very few individuals per site or system. Wherever possible, control of these systems must reside with the MIS Staff or GSA.

11.1.2 Securing Offices, Rooms, and Facilities

All offices, rooms and facilities that contain other than public information resources will be protected accordingly to prevent unauthorised access, damage or interference to the business processes.

11.1.2.1 Site Assessment

A site assessment of secure areas to determine the type of control that is appropriate and prudent, taking into account not only personnel risks, but also that of environment, neighbourhood, civil unrest, and natural and man-made disasters shall be conducted. Health and safety regulations and concerns will also be examined and controls incorporated. Resulting policies should vary greatly depending on the locality of the office (i.e. Malaysia verses Thailand).

Information processing facilities that are managed by third party organisations shall be separated from those that are managed in-house.

11.1.2.2 Securing Sites when Unoccupied

Rooms in facility that contain sensitive assets shall be locked when not in use. Windows and doors shall be kept locked and have protection from intrusion or environmental factors. Intrusion alarms should be in place and maintained to the vendors' standards as applicable according to the information protection requirements (see 9.2).

Sensitive documents shall be locked in file cabinets or other protective furniture that takes into account the results of the risk analysis.

Additional controls shall be implemented for computer and communications rooms or areas. Key facilities shall be situated so as they avoid public access. Support functions and equipment should be situated in a way that keeps them away from the public and unauthorised personnel.

11.1.2.3 Signage and Directory Listings for Secure Sites

The uses of buildings that contain sensitive materials or processing facilities will be unobtrusive and not marked in such a way that gives the public and indication of their purpose or function.

Directories and telephone books that provide information on locations of sensitive facilities shall be secured from unauthorised access.

11.1.2.4 Monitoring of Facilities for Physical Security

Where possible, systems shall monitor the physical security of facilities. Monitoring could include any or all of the following technologies, based on the outcome of the physical security assessment:

a. Closed circuit TV or video cameras
b. Glass break sensors
c. Door and window opening alarms
d. Hold open sensors for doors or windows
e. Above or below ceiling sensors (sites with false ceilings and walls that do not extend from floor to ceiling
f. Security Patrols

11.1.3 Other Site Security Issues

Hazardous or combustible materials shall be stored securely a safe distance from secure facilities. Only necessary bulk supplies shall be stored within secure facilities.

Back-up equipment and media shall be stored off-site and a safe distance from facilities sufficient that it would not be damaged if the facility is damaged.

12.0 COMMUNICATIONS AND OPERATIONS MANAGEMENT

12.1 Operational Procedures and Responsibilities

12.1.1 Documented Operating Procedures

All standard operating procedures should be formally documented and maintained to ensure the correct and secure management of all information processing facilities.

Formal documented procedures and detail execution instructions will be in place for each job, including, but not limited to:

a. Information processing and handling;
b. Scheduling requirements including system interdependencies and prioritisation;
c. Instructions for error handling, during job execution;
d. Instructions for exceptions during job execution;
e. Restrictions on the use of system utilities (see 9.5.5);
f. Operational and support contacts for technical difficulties;
g. Output instructions for confidential or sensitive output;
h. System restart and recovery procedures in the event of system failure;
i. Housekeeping functions in information processing facilities such as start-up and close down, equipment maintenance, computer room and mail management and safety; and

Formal authorisation from management will be obtained prior to any changes to documentation.

12.1.2 Operational Change Control

Formal management responsibilities and procedures to control all changes to equipment, software or procedures shall be established and followed for change, integrating operational and application change control procedures (see 13.3.1), and logging all changes.

There shall be a formal approval for proposed changes (that could potentially impact the computing environment) that will be developed by the development team.

Prior to any operational change there shall be an assessment that:

a. Identifies significant changes;
b. Records significant changes;
c. Assesses the potential impact of such changes; and
d. Procedures and responsibilities for aborting and recovering from unsuccessful changes.

All changes shall be communicated to all relevant persons. The system owner shall manage this process with the assistance of the GSA and/or lead person from development team.

12.2 Information System Planning and Acceptance

12.2.1 Capacity Planning

To limit disruption to the network, applications, and business functions, GSA will monitor information system capacity and plan for future capacity needs in sufficient time to procure system resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

System owners shall monitor their usage for current uses and projected capacity.

12.2.1.1 Provisioning of Hardware and Software

Group MIS must be consulted whenever deploying any new systems for adequate provisioning of system hardware and software to take advantage of any contracts or discounts that may be in place. Group MIS will obtain and install the equipment, as appropriate, and then allow access to the appropriate user group for use of the equipment. Provisioning of software requires purchasing of any applicable licenses for use (see 14.1).

12.2.1.2 Management of Network Storage

To allow adequate storage capability to support all users, Group MIS shall monitoring and managing online and offline storage capacity. These will include types or classes of storage, data backup (see 12.4.1), protection by information classification (see 9.2.1), and any quotas necessary based on the business reasons for storage. GSA who in-charge of storage will incorporate any requirements given in information retention (see 9.3).

12.2.2 System Acceptance

To ensure new systems or applications do not disrupt the network, existing applications, or other systems, a system acceptance process will be defined. This process will document acceptance criteria for new systems prior to acceptance. All systems will be tested prior to acceptance, including a vulnerability assessment or scan prior to being permitted to connect to the INGRESS network. This process will ensure that security controls are in place and that the new system complies with the design and function required.

System owners shall ensure that the usage capacity requirements are met prior to use of new system (see 12.2.1).

System owner (when applicable) shall inspect major new systems periodically throughout the development to ensure functionality is appropriate and compliant with design requirements.

Prior to the acceptance and use of new systems the following controls shall be documented and in place:

a. The system is built according to standard hardware or software builds,
b. Effective manual contingency procedures are documented (if applicable)
c. Error recovery/restart procedures and contingency plans (if applicable)
d. Updated business continuity plans (if applicable)
e. Compatibility of new system to the information security requirements in INGRESS
f. Compatibility of the new system to the existing systems
g. Information Security controls are in place and tested
h. Vulnerability scan run against system to verify that patch levels are current and that no unnecessary services are running.
i. Users shall be adequately trained prior to taking a new system into operational mode.

Operational testing procedures shall be documented and preparation for new system completed prior to acceptance. Systems must meet acceptance criteria, or have formal exceptions authorised, before being connected to the INGRESS network.

Note that these requirements do not apply to any system not connected to the INGRESS corporate network. This includes stand-alone systems, or systems in isolation and not connected to the rest of the network. If these systems are subsequently brought out of that environment and the desire is to connect them to the INGRESS network, then these requirements apply once again.

12.2.2.1 Network Infrastructure Services on the Production Network

Network infrastructure services, such as Domain Controllers, DNS servers, DHCP servers, or other similar services will not be deployed on the production network except by GSA. If other departments require these services for projects, they must request these services to be deployed by GSA, and these services must be configured to not interfere with the existing infrastructure of the network. There is no restriction in deploying these services on isolated networks.

12.2.2.2 Third Party Systems on the INGRESS Network

If partners or vendors require placement of their devices on the INGRESS network, special acceptance criteria must be applied. Third party devices must meet all system acceptance criteria as if they were INGRESS systems, in addition to special access to the network. INGRESS may not necessarily have physical or administrative control of the systems, so mitigating network controls must be also put in place.

Third party devices must be restricted in the access they may have on the network. This should be implemented through the use of Access Control Lists on the closest network device or other similar technologies. Third party systems should be placed on an 'island' or other segregated network segment allowing only specific data (required by the business) transferred between that network and the rest of the INGRESS network.

The placement of such devices must be approved by the HGM and the GSA before the device may be connected.

12.3 Protection Against Malicious Software

This policy will protect the integrity of software and information by promoting procedures and user actions to mitigate the risks of the introduction of malicious software into the organisation.

To prevent interrupted service caused by computer viruses for both computers and networks, all personal computer users must keep current versions of approved virus-screening software enabled on their primary computers at all times.

INGRESS shall comply with the requirements of software licenses. No unauthorised or illegal software will be used. See also 14.1.2.

All e-mail attachments will be scanned when entering the network or server scanned prior to use. All unauthorised files or amendments will be thoroughly investigated.

Procedures and responsibilities for the use of, training in, reporting on and recovery of virus attacks will be developed and documented. All users will receive training on virus awareness and virus control procedures (see 8.3). Business contingency plans shall include the handling and recovery from virus attacks.

12.4 Housekeeping

12.4.1 Information Backup

INGRESS will regularly back-up adequate copies and generations of all software, documentation and business information and store it off-site. Restoration testing shall be done to ensure the quality and usability of backed-up resources. The purpose of this policy is to maintain the availability and integrity of information resources in the case of failure or disaster, by retaining up-

to-date back-ups that are stored at a distance sufficient to escape damages that might occur at the main site.

a. Restoration procedures will be documented and tested to ensure that they are effective and comply with restoration time requirements. Restoration procedures shall be kept with the back-up copies at the remote location.
b. The back-up site shall implement similar physical and environmental controls as the ones in place at the main site (see 10.0).
c. Back-up media shall be tested semi-annually to ensure the back-up can be relied upon. GSA shall be responsible for ensuring that back-ups are tested.
d. Retention schedules will be adhered to for all business information.

12.4.1.1 PC Data Backup

To protect INGRESS's information resources from loss or damage, personal computer users are responsible for regularly backing-up the information on their personal computers to their respective network file shares storage that are assigned to them by the MIS Staff. These shares are backed up daily to secure media for disaster recovery purposes.

12.5 Network Management

12.5.1 Network Controls

Group MIS shall implement strict controls on INGRESS's networks to ensure the safeguarding of information and protection of INGRESS's infrastructure. Controls shall guarantee the security of data in networks and protect the connected services from unauthorised access. All procedures and responsibilities will be documented. Network access controls will be observed for networks connected to public networks (see 10.4).

The GSA should closely coordinate the controls on INGRESS's networks to assure functional optimisation as well as consistency of controls.

12.5.2 Production of SPAM

INGRESS staff shall not produce Unsolicited Commercial E-mail (otherwise known as SPAM) to be sent out to the Internet. Any commercial e-mail should be specifically targeted to recipients in accordance with applicable laws and regulations (see 14.1). If allowed mass e-mailings will be made, Group MIS will be consulted to determine the effects of these mailings on systems and the network, and appropriate mitigation efforts will be enacted (such as system, time of day, or network path restrictions).

12.6 Vulnerability Management

Effective vulnerability management can reduce risk to INGRESS's computing environment by verifying that systems or network devices are using current up to date patch levels, are not running unnecessary services, and do not have default passwords.

Group MIS shall run internal vulnerability scans against any systems containing (or accessing systems that contain) confidential data at least on a bi-annually basis.

Group MIS shall conduct with a trusted third party to run external vulnerability scans against any Internet-facing systems on at least a bi-annually basis.

13.0 SYSTEMS DEVELOPMENT AND MAINTENANCE

13.1 Security Requirements of Systems

13.1.1 Security Requirements Analysis and Specification

The purpose of this policy is to ensure that all new systems comply with the organisation's security requirements. Security approval shall be required for all key project phases (i.e. concept, requirements, testing). All new or upgraded systems must have their security requirements documented.

a. An assessment shall be performed to evaluate the security requirements for new systems or upgrades.
b. The system owner, in conjunction with the HGM, shall specify the security requirements of all new implementations prior to their final approval.
c. The controls and requirements should reflect the sensitivity and business value of the information assets involved.
d. Independent consultants may be brought in to assist in evaluations if deemed necessary.
e. Vulnerability scans and/or penetration tests should be run against systems to ensure security controls are in place, patch levels are current, and unnecessary services are not running.

13.2 Security in Application Systems

13.2.1 Input Data validation

All applications should validate input data before storing or processing. This will ensure that the data input to systems is correct and appropriate, therefore protecting the integrity of the organisation's information systems.

a. Checks shall be applied to all standing data inputs (i.e. names, addresses).
b. Checks shall be applied to parameter tables (i.e. material or product codes).
c. Dual input or other input checks shall be used to detect:
    i. Out of range values
    ii. Invalid characters in data fields
    iii. Missing or incomplete data
    iv. Exceeding upper or lower data volume limits
    v. Unauthorised or inconsistent data control
d. There shall be procedures for testing the plausibility of data inputs.
e. A periodic review of the content of data in key fields will be done to confirm validity and integrity of data. Procedures shall be put in place to respond to validation errors.
f. All users shall be trained on their responsibilities involved with input as well as how to respond to input validation errors.

13.2.2 Control of Internal Processing

Mitigation of internal processing risks will be accomplished by incorporating validation checks into systems that will detect corruptions from processing errors or vandalism. These controls will protect the integrity of the organisation's information systems by building security into the organisation's application systems and by ensuring the data run through the systems is complete, correct and appropriate.

Prior to implementation, system owners should ensure that applications are designed and implemented with restrictions that minimize the risk of processing failures that would undermine the integrity of the organisation's information.

Controls will be in place to:

a. Manage the location and use of add and delete functions to change data
b. Prevent programs from running in the wrong order
c. Prevent programs from running after a prior processing failure (see 12.1.1)
d. Ensure the use of correct programs to recover from failures and ensure the correct processing of data
e. Other actions to protect the integrity of application systems may include:
    i. Performing system or batch controls to reconcile data file balances after transaction updates,
    ii. Instituting balancing controls to check opening balances against previous closing balances,
    iii. Validating system-generated data (see 13.2.1),
    iv. Performing checks on the integrity of data or software that is uploaded or downloaded, as applicable. Hash totals of records and files may be maintained,
    v. Performing checks to ensure that applications are run at the correct time order and terminate in case of failure.

13.2.3 Output Data Validation

All output of data from application systems will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

a. Output data shall be checked for plausibility and reasonableness.
b. Output data counts shall be reconciled to ensure all data was processed.
c. Output data shall provide the reader with enough information that they can determine accuracy, completeness, precision and data classification (see 9.2).

Application owners will document procedures for responding to output validation tests and user responsibilities and will ensure that all users are trained on output validation policies and procedures.

13.3 Security in Development and Support Processes

13.3.1 Software Change Control Procedures

Software development at INGRESS shall utilise formal change control procedures for any changes to software. This process shall be integrated with the operational change control procedures (see 12.1.2). The purpose of this policy is to ensure that the security, availability and integrity of system software, systems and information are not compromised when there are changes to software.

The application owners shall be responsible for overseeing the security and control procedures of all changes to their applications. All software changes require formal approval by the application owner. All changes to software will be documented.

Application owners shall be responsible for insuring that programmers are only given access to areas of the application that are necessary for the approved work.

Application owners shall oversee the entire application change process prior to change including:

a. Maintaining a record of agreed upon authorisation levels,

b. Ensuring changes are submitted by authorised users,
c. Performing risk assessment to assure that controls and integrity procedures will not be compromised by changes, that business interruption is kept to an acceptable minimum and that the timing is appropriate for the change,
d. Identifying all software, information, databases and hardware that require change,
e. Obtaining formal and detailed proposals and specifications before work commences,
f. Obtaining formal approval prior to work commencing,
g. Application owners shall oversee the entire application change process during the change, including:
    i. Ensuring change minimised business interruption,
    ii. Documentation is updated and old documentation is archived,
    iii. Version control is maintained,
    iv. Maintaining an audit log of all change requests,
    v. Updating all user procedures,
    vi. Ensuring that users accept all changes prior to implementation,
h. Application owners shall oversee the entire application change process after the change, including:
    i. Ensuring that testing is done securely (in a test environment that is segregated from development and operational systems)
    ii. Ensuring that implementation does not disrupt business processes

13.3.1.1 Patch Management Process

Group MIS will institute a Patch Management process for operating systems and commercial software that will include the following elements:

a. Identification of new patch availability
b. Assessment of applicability and criticality of patches
c. Patching effort timing and methods
d. Effects of patches on existing applications
e. Testing of patches before deployment
f. Documentation of patch levels for various systems and applications

13.3.2 Technical Review of Operating System Changes

Group MIS shall review and test all new operating system changes or updates prior to installing them in an operation environment. This will ensure that operational integrity is maintained and that the organisation's security requirements are met by any new operating system release.

An assessment shall be performed prior to the change of any of the organisation's operating systems that shall include:

a. Application control and integrity procedures – will they be compromised by operating system changes?
b. Annual support plan and budget – will this cover testing of the new operating system?
c. Timing of change – is there enough time to thoroughly test and review new operating system changes?
d. Business continuity plans – have they been modified to accommodate changes.
e. Whenever possible, operating systems shall be maintained at a level supported by the vendor.

13.3.3 Restrictions on Changes to Software Packages

To ensure integrity and security of vendor supplied software packages, as well as to minimize the expense and support issues associated with modified products, INGRESS will use standard, unmodified vendor supplied software programs whenever possible.

If modifications must be made, the organisation shall do an assessment to clarify and control the following issues:

a. Compromise of built in controls and integrity processes,
b. Vendor requirements for consent,
c. Impact of future maintenance (Is vendor support still available or will the organisation be responsible?)
d. Whenever possible the organisation shall request that the vendor makes changes part of a future standard release,
e. If changes must be made, an original copy of standard software shall be retained and the changes clearly documented in the operational copy,
f. All changes shall be thoroughly tested prior to use,
g. All changes shall be clearly documented in case there is a need to reapply the changes.

13.3.4 Covert Channels and Trojan Code

To prevent damage to INGRESS systems and applications, INGRESS will actively protect its information assets from covert channels and Trojan code.

The organisation shall follow the following procedures when acquiring software:

a. All programs shall be a acquired from reputable sources
b. All programs should be acquired in source code (if available)
c. All programs that are acquired should have source code verified
d. All products should have source code inspected prior to operational use
e. All programs that are acquired shall be evaluated products
f. Access shall be that which is allowed in this policy (see 10.1).

Modification to code, if necessary, shall be controlled, monitored, inspected, and only done by those staff members that have proven their trustworthiness to work on key systems.

14.0 COMPLIANCE

14.1 Compliance with Legal Requirements

14.1.1 Identification of Applicable Legislation

To avoid any legal or security breaches, INGRESS will define, document, and comply with all relevant statutory, regulatory, and contractual requirements for each information system.

Each system owner shall implement controls to comply with all relevant statutory, regulatory and contractual requirements for their information system.

System owners shall seek the advice of the Legal or Group MIS for all relevant legal and security information.

Care shall be taken to account for different requirements in different locations (i.e. Malaysia, Thailand and Indonesia). INGRESS's Legal Officer will determine differences from standing policy for those locations that have differing legal requirements, and will work with the HGM to create exceptions to general policy and specific policies for those jurisdictions.

14.1.2 Intellectual Property Rights

All users at INGRESS will comply with the legal aspects of intellectual property protection and the rights and limitations of license agreements associated with proprietary software products.

The purpose of the policy is to ensure that users are aware of and comply with such restrictions as copyrights, trademarks, and design rights. Users are responsible for not violating applicable copyright, intellectual property, or other licensing rights of electronic media or software that is not the property of INGRESS. Furthermore, users are responsible for not using INGRESS intellectual property outside the limits of INGRESS policy or licensing.

Failure to abide by these policies will subject the user to disciplinary actions up to and including termination or criminal/civil charges.

14.1.2.1 Intellectual Property Standards and Training

Intellectual Property Rights Protection policies shall be included in all security awareness training (see 8.2).

HGM and/or GSA, along with each system owner, shall establish, document and educate applicable users on:

a. Maintaining appropriate asset registries,
b. Maintaining proof of ownership or licenses,
c. Implementing controls to restrict the amount of users to the appropriate licensed amount,
d. Implementing controls and checks to ensure that only licensed software is installed,
e. Procedures and controls to assure that license conditions are met,
f. Procedures and controls for disposing of or transferring software to others,
g. Use of appropriate audit tools,

14.1.2.2 Using Software from Outside Sources

a. Users shall not download or install any third party pirated software on INGRESS systems.

b. Users shall not download or install any non-approved software from the Internet.
c. The GSA to approve specific software for use from the Internet if there is a business need.

14.1.2.3 Copyrighted Material and Peer-To-Peer File Sharing

INGRESS respects the copyrights of those involved in creating and distributing copyrighted material, including music, movies, software and other literary and artistic works. It is the policy of INGRESS to fully comply with all copyright laws.

INGRESS provides its employees access to computer systems and the Internet to allow them to do their jobs on behalf of INGRESS. Employees may make occasional use of the Company's computer systems and network for personal use.

When INGRESS employees need to use copyrighted materials to do their jobs, INGRESS acquires appropriate licenses.

INGRESS employees shall not:

a. store or otherwise make unauthorised copies of copyrighted material on or using INGRESS computer systems, networks or storage media;
b. download, upload, transmit, make available or otherwise distribute copyrighted material using INGRESS's computer systems, networks or storage media without authorisation; or
c. use or operate any unlicensed peer-to-peer file transfer service using INGRESS's computer systems or networks or take other actions likely to promote or lead to copyright infringement.

Please note – this is not a policy against MP3 files, or electronic music and video files as such. Rather, the policy is targeted at unauthorised – that is, unlicensed – electronic music and video files. If you downloaded the files from an unlicensed peer-to-peer site (i.e., Morpheus, Grokster, KaZaA, etc.) or other source, then those files are almost certainly not authorised and most likely violate the copyright laws.

INGRESS reserves the right to:

a. Monitor its computer systems, networks and storage media for compliance with this and other INGRESS policies at any time, without notice and with or without cause; and
b. Delete from its computer systems and storage media, or restrict access to, any unauthorised copies of copyrighted materials it may find, at any time and with or without notice.

14.1.3 Data Protection and Privacy of Personal Information

INGRESS should comply with all applicable laws and regulations regarding the protection of personal data. This will ensure that INGRESS is collecting personal information (that information that can be used to identify living individuals) in a manner that complies with laws as well as processing and disseminating that data in a lawful manner.

a. HGM or a nominated Group MIS staff should document policies and procedures that comply with applicable laws and regulations for the handling of personal information for each such instance.

b. Group MIS shall distribute policies and educate users, managers and service providers on their responsibilities for compliance.

c. Information owners shall inform the GSA about proposals to keep information in a structured file. GSA shall advise information owners on policies and procedures concerning their protection and storage of such data.

d. Confidential information entrusted to INGRESS by members, business partners, suppliers, and other third parties shall be protected in accordance with this policy and shall be protected with at least the same care as INGRESS's confidential information.

14.1.4 Prevention of Misuse of Information Processing Facilities

Users of INGRESS information processing facilities will utilise these facilities for only management-authorised business purposes. INGRESS reserves the right to legally monitor facilities for compliance. The purpose of this policy is to protect the availability and integrity of the organisation's information processing facilities as well as protect the organisation against legal sanction against the misuse of computers.

a. HGM shall provide managers with guidelines for the legal monitoring of computer facilities.

b. GSA shall monitor the use of such facilities.

c. If misuse is detected, it shall be brought to the attention of the person's manager for disciplinary action.

An acceptable use policy will be communicated to users. This policy will be included in the acceptance of policy letter that employees will sign during orientation. The acceptable use policy will govern permitted and forbidden activities for their location. In all cases, any activity not expressly permitted is forbidden.

14.2 Reviews of Security Policy and Technical Compliance

14.2.1 Compliance with Security Policy

a. To maintain the security, integrity and availability of the organisation's information processing assets, INGRESS will continually monitor the organisation's compliance with its security policies.

b. HGM shall ensure that an annual internal audit takes place. The scope of this audit is a Security Posture assessment for all external/internal routers, firewalls, access points, hosts and offsite facilities for Disaster Recovery and media storage.

c. Head of Business Unit or representative shall continually monitor their user's compliance with the organisation's security policies, procedures, standards and requirements (for information on monitoring see 10.7).

14.2.2 Technical Compliance Checking

a. GSA shall monitor the organisation's technical compliance with its security implementation standards.

b. A specialist shall be used for technical compliance checking to ensure that hardware and software security controls have successfully been implemented in operational systems.

c. The technical compliance checking will be done manually by the MIS Staff, with automated software tools or in combination.

d. A qualified technical specialist shall interpret results of subsequent technical reports.

e. Penetration testing shall be done annually or as necessary (care shall be take that a successful penetration test does not compromise they system or exploit other vulnerabilities).

f. GSA shall oversee all technical compliance testing.

14.3 System Audit Considerations

14.3.1 System Audit Controls

Any agency conducting system audits will carefully plan, agree upon, and expedite system audits so as to minimize the risk of disruptions to operational business processes. This will ensure the organisations security requirement compliance while maximizing the availability, integrity and security of the organisation's information resources.

a. The scope and requirements of all audits shall be controlled and agreed to by management.

b. Access to any files beyond read only shall be approved by the HGM. This includes isolated copies of system files. If isolated copies of system files are used, the files shall be destroyed as soon as the audit is completed.

c. Requirements for additional testing shall be identified and agreed upon by appropriate management.

d. Information resources shall be identified and made explicitly available for audit assistance.

e. All access to system shall be logged to produce a reference trail.

f. All procedures, responsibilities, requirements and scope shall be documented.

14.3.2 Protection of System Audit Tools

Any agency conducting system audits will protect access to system audit tools (i.e. software or data files). This will protect the security, availability and integrity of the organisation's information resources by ensuring that the organisation's system audit tools are protected from misuse or compromise.

System audit tools shall be separated from operational and development systems unless they are given the added appropriate protection and are authorised by the HGM.

Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance by HGM or GSA (see 8.3.2).