INFORMATION SECURITY POLICY

(GIT-POL01)

Gamuda Berhad

Menara Gamuda, PJ Trade Centre, No.9, Jalan PJU 8/8A, Bandar Damansara
Perdana, 47820 Petaling Jaya, Selangor

PREPARED BY	CHECKED BY
[signed]	[signed]
FAEEZA BINTI MOHD NOOR IT GOVERNANCE AND COMPLIANCE	JOHN LIM JI XIONG CHIEF DIGITAL OFFICER

APPROVED BY
[signed]
CENTRE OF EXCELLENCE COMMITTEE

REVISION HISTORY

DATE	REV.NO.	PAGE	DESCRIPTION
13/02/2017	00	All	Original documents
03/07/2023	01	All	Upgrade to ISO/IEC 27001:2022
17/10/2023	02	13	2.0 Information Security Policy Statement - amendment made based on findings from Stage 1 CB Audit.

TABLE OF CONTENTS

1.0 GENERAL

This Information Security Policy provides the Gamuda Group employees and third parties with a consistent set of security rules required to protect the company's information, information assets and intellectual property.

The rule set forth in the Policy document has been defined to provide reasonable controls for protecting the company from a wide variety of security threats which could cause harm to Gamuda Group business activities. Defining and implementing Policy are one of the security layers that need to be put in place in order to safeguard the organization from traditional and cyber threats and vulnerabilities.

1.1 Definition of the Policy

The information security Policy is the management instructions indicating a course of action, a guiding principle, or an appropriate procedure, which is expedient, prudent, or advantageous. This Policy high-level statements that provide guidance to the organizational activities.

Policy(s) are mandatory. View it as the equivalent of an organization-specific law. Hence compliance with a control practice is required.

Policy(s) are also different from 'procedure'. A Policy statement describes the general means for addressing a specific problem (a 'high-level approach') and should not become detailed and lengthy.

1.2 Scope of the Policy

This document deals with Information Security issues related to the corporate environment of the company, i.e. any activity that protects information and/or information assets of the company. The control practice apply to the security principles of confidentiality, integrity, and availability of information obtained, created, or maintained by the employees or non-employees (third party's) accessing the company information asset.

2.0 INFORMATION SECURITY POLICY STATEMENT

It is the policy of Gamuda Group to ensure that information is properly managed, appropriately secured and protected against the consequences of breaches of confidentiality, failures of integrity or interruptions due to the availability of that information. The Management of Gamuda Group is committed to ensure that:

- The confidentiality of information is protected to prevent disclosure of valuable or sensitive information;

• Information is available with minimal disruption to authorised users to meet client's and business' requirements;

• The integrity of information is maintained to ensure its accuracy and completeness; • Information Security education, awareness and training will be made available to users to ensure responsible participation;

• All breaches of information security, actual or suspected, will be reported. All users must understand their roles and responsibilities in handling incidents;

• Information Security Risks, Cybersecurity Risks and Data Privacy Risks are mitigated to an acceptable level through an Information Security Risk Management Framework;

• Appropriate security & permission controls will be jointly maintained by Group IT, respective Business Units and parties who are related to the Group either internal or externally;

• Appropriate resources are allocated in order to implement, operate and review an effective Information Security Management System;

• Disruption to information processing facilities will be minimised. Readiness should be ensured via regular testing based on prevailing risks; • Regulation and legal requirements on Information Security related to The Group are met; and

• The Information Security Management System is continually improved.

The Group shall follow a formal disciplinary process for employees who have allegedly violated the information security policies and procedures.

3.0 INFORMATION SECURITY MANAGEMENT OBJECTIVES

The purpose of Information Security Management is to protect all information assets of Gamuda Group, either electronic or paper, from all threats, whether internal or external, deliberate or accidental.

Gamuda Group through implementation of ISMS will ensure the following objectives:

- To protect Information Assets (digitized or paper) against unauthorised access or disclosure through deliberate or careless action
- To ensure Integrity of information through protection from unauthorised modification
- To ensure availability of information to authorised users when required
- To safe guard IT Systems in support of business operation through effective controls
- To comply with all Contractual, Regulatory and Legislative requirements
- To allocate appropriate level of Information Security in the job responsibilities
- To provide information security awareness and training to all employees

- To investigate and report and handle information security incidents

The intention of Gamuda Group is to implement ISMS within the IT department. The detail scope of ISMS, specification and boundaries is further defined in the ISMS Manual.

Selection of the scope is based on IT department business-critical functions in Gamuda Group. This is complemented with the level of Confidentiality, Integrity and Availability of information in each business services.

4.0 RESPONSIBILITIES

The IT Governance Unit has direct responsibility on the overall maintenance of the information security Policy and providing advice and guidance on implementation and directly responsible for maintaining the codes and providing advice and guidance on company implementation.

The Units Heads in IT department are directly responsible for implementing the policy within their business areas, and for adherence by all their staff.

Staff should know, understand, and be held accountable for fulfilling their information security responsibilities.

5.0 INTENDED AUDIENCE

1. All employees of IT Department, Gamuda Group
2. Authorized Third Party (with authorization from relevant Units Heads)

Any person(s) not listed above are not authorized to examine the contents of this document. Doing so would constitute a breach of security that may be subjected to appropriate actions being taken against the offender.

6.0 COVERAGE OF THIS DOCUMENT

This ISP statement covers the full range of Policy statements in mitigating risks associated with creating, amending, storing or disseminating information. This document consists of information security domains related to:

1. Information Security Policy Statement
2. Organization of Information Security
3. Information & Processing Devices Asset Management
4. Information Security related to Human Resources
5. Information Security related to Physical and Environmental

6. Information Security related to IT Operations & Network
7. Information System Access Control
8. Information System Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Information Security related to Business Continuity Management
11. Information Security related to Legal and Contractual Compliance

7.0 HOW TO READ THIS CONTROL PRACTICE STATEMENTS

Each of the areas consists of at least one (1) security objective, and each security objective consists of at least one (1) policy statement.

Example:

ISP-060106 Contact With Authorities	
There shall be appropriate contacts with information service providers and telecommunication operators, enforcement authorities such as Police, Cybersecurity Malaysia to ensure that appropriate action can be quickly taken and advice obtained, in the event of a information security incident.	ITGC

ISP Statement

Group / Individual

Explanation:

ISP	:	**Information Security Policy**
060106	:	The first two digits are for the major topic number, second two digits are for the security objective, and third two digits are the policy number.
ISP Statement	:	The description of the ISP statement.
Group / Personnel	:	The personnel or group of people affected by the policy statement, who may be considered as owners of specific policy statements.

DOMAIN 01 - INFORMATION SECURITY POLICY STATEMENT		
Objective: Information Security Control Statement		
Description	To provide management direction and support for information security.	
ISP-010101	**Endorsement for Policy**	
	This Policy shall be approved by the Chief Digital Officer	ITGC
ISP-010102	**Maintenance Role**	
	The maintenance and review of this Policy is by GIT with coordination of ITGC.	GIT, ITGC
ISP-010103	**ISP review**	
	The ISP shall be reviewed and maintained periodically in response to any changes affecting the basis of the original risk assessment, periodic audit or in response to requests from within the organization. At a minimum a comprehensive annual review must be carried out. The periodic review may include the following: 1. The policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents, 2. Cost and impact of controls on business efficiency, and 3. Effects of changes to technology.	GIT, ITGC
ISP-010104	**Exception to ISP**	
	If an exception is required for ISP, a written request which includes a description of and justification for the exception/change should be brought forward to ITGC for approvals. ITGC should retain all such requests, for future reference.	ALL, ITGC
ISP-010105	**User awareness on ISP**	
	The ISP must be communicated throughout Gamuda Group to employees in a form that is relevant, accessible and understandable to the intended readers.	Training, ITGC, GIT and Project Owner

	Training Unit is responsible in arranging and coordinating for new recruits on this ISP also The Training Unit is responsible in arranging and coordinating a yearly refresher awareness program on ISO related policies and procedures for existing users. For communication to external parties - the respective Project Owner is responsible to make aware on relevant control practice in this ISP to third parties.	
ISP-010106	**Enforcement of ISP**	
	Employees are advised to observe the rules and take initiatives in supporting organization efforts. The Unit Heads are responsible in enforcing the ISP throughout his/her jurisdiction.	All Unit Heads

DOMAIN 02 - ORGANIZATION OF INFORMATION SECURITY		
Objective: Information Security Infrastructure		
Description	To establish a management framework for the implementation of information security within Gamuda Group and to assign roles and responsibilities for the management of information security.	
ISP-020101	**Information Security is every employee’s duty**	
	All employees of Gamuda Group must review, understand and comply with their information security responsibilities. Should employees unclear on their responsibilities they are responsible to seek clarification from their superior. All employees are required to protect Gamuda Group information assets (i.e. information, resources, and reputation).	ALL
ISP-020102	**Centralized management of Information Security**	
	Guidance, direction and authority for detailed implementation of information security activities are centralized for Gamuda Group within ITGC and GIT.	ITGC, GIT
ISP-020103	**CDO responsibilities (information security-related)**	

	The CDO is responsible to: 1. Provide clear direction to the overall Information security implementation with the advice of Head of ITGC 2. Ensure all information security control practice, standards and procedures are established, enhanced and complied with at all times.	CDO
ISP-020104	**ISMS Committee responsibilities (information security-related)**	
	The ISMS Committee comprises of Information Security Management Representative (ISMR) and Committee Member. The committee is responsible to: 1. Define Gamuda Group information security goals 2. Formulate appropriate information security control practice to reach the goals 3. Evaluate results of information security risk management program 4. Review major Information Security Incidents. 5. Evaluate results of security effectiveness program periodically 6. Perform management review for Information Security Management System at least once a year in accordance to the relevant clauses in ISO 27001	ITGC, ITAM
ISP-020105	**IT Governance responsibilities (information security-related)**	
	The IT Governance and Compliance of GIT is responsible to: 1. Provide input and influence over the direction of the information security program. 2. Set and recommend priorities on information security efforts. 3. Recommend to the ISMS Committee on information security projects in reducing the organizational information security risk through implementation of acceptable controls.	ITGC

	4. Monitor deliverables produced through the information security program. 5. Conduct review of the ISP, supporting procedures, and review of the implementation and subsequent enforcement of the policies. 6. Discuss and identify probable improvement on the practical ability to support the ISP. 7. Establish buy-in for subsequent support of implementation activities. 8. Monitor effectiveness of security controls and information security risk mitigation within ISMS implementation.	
ISP-020106	**Group Information Technology (GIT) responsibilities (information security related)**	
	The GIT has primary responsibilities for the day-to-day management of Gamuda Group technological information security processes. The following are the responsibilities of the GIT. 1. Oversee the administration of logical access controls. To ensure adequate access controls are implemented on new system or during system maintenance based on Business Owner's requirements. GIT is responsible on the Group level for the administration of logical access controls for all IT system and monitoring access violation based on Business Owners initiation and approval. 2. Provide advice and guidance on the development, maintenance and implementation of ISP. 3. Providing technical and operational management support for a wide variety of information system projects and activities. 4. Configuring and updating workstations, servers, networks, and other information system equipment used in support of business Gamuda Group activities. 5. Maintain system in a corrective and preventive manner, so that all applications critical to the business are adequately supported, so that	GIT

	response time and availability is within tolerable limits, and that security vulnerabilities are minimized. 6. Manage third parties and relevant contracts providing services to develop, support, or maintain hardware and system to achieve the above objectives. 7. Provide a central point to track and escalate system problems and incidents, as well as to ensure timely responses for resolutions. 8. Review adequacy of the IT Disaster Recovery Plan (DRP) to allow recovery from a system failure and in the event of a disaster resulting in a loss of the information technology services. 9. Assurance of the monitoring on the supply of electricity to Data Centre. 10. Assurance on the maintenance of fire extinguisher, fire suppression system for work areas and Data Centre.	
ISP-020107	**Risk Management responsibilities (information security related)**	
	The following are the responsibilities that to be taken: 1. Coordinate and ensure the Risk Management and Mitigation for information security are satisfactorily implemented by all departments within the scope of ISMS in Gamuda Group. 2. Review adequacy of the Business Continuity Plan (BCP) to allow recovery and in the event of a disaster resulting in a loss of business services. 3. Provide advice and guidance on the development, maintenance and implementation of Risk Management and Business Continuity Plan. 4. Governance of documentation for ISO related	ITGC
ISP-020108	**Legal responsibilities (information security related)**	
	The following are the responsibilities that to be taken:	ITGC

	1. Providing necessary advice to conduct Gamuda Group business activities in a manner fully in comply with existing laws and regulations. 2. Providing advice on compliance, regulations and contractual relationships that can be used to further Gamuda Group business interests. 3. Providing Gamuda Group with advice against legal risks to appropriately protect Gamuda Group information assets, resources and employee. 4. To ensure the monitoring and compliance to Personal Data Protection Act for Gamuda Group.	
ISP-020109	**Human Resource and Admin responsibilities (information security related)**	
	The following are the responsibilities that to be taken: 1. Screening on new recruits in relation to the job placement as to minimize threats from them in protecting organization information assets. 2. Provide administrative support to keep and maintain the records needed to be in compliance with all human resources related laws, regulations and internal policies, and 3. Coordinate the retention and termination of all Gamuda Group employees and return of assets. The Infra unit is responsible with the following: 1. Assurance on the preservation of information security at the record storage centre via Crown Records. The Admin department is responsible with the following: 1. Ensure the security and physical access control for Gamuda Group. 2. Administration, management, installation, monitoring and review CCTV images.	GHR INFRA UNIT ADMIN DEPARTMENT

	3. Access control and the use of card access for physical access control to Gamuda Group buildings via card system.	
ISP-020110	**IT Procurement and Asset Unit responsibilities (information security related)**	
	The IT Procurement and Asset Unit is responsible to: 1. Ensure the IT Procurement Process as per the IT Procurement Procedure. 2. Ensure selected vendors adhere to Gamuda Group NDA.	ITAM
ISP-020111	**Information Asset ownership and management's responsibilities**	
	All Information & Processing assets used by each unit/department must have a designated owner. Employee must aware the asset owners and assigning responsibility for the control of asset.	ALL
ISP-020112	**IT asset inventory**	
	IT will maintain accurate inventory records of all IT assets procured by the company. Information recorded includes date of purchase, price of item, name and address of vendor, warranty period etc. IT will maintain accurate assets records of all current location and individual or department to whom the asset has been assigned. Information recorded includes date of purchase, price of item, asset identification number, name of asset, name and address of custodian. All inventory records will be maintained and monitored in an inventory system. Information assets and processing related assets will be documented.	ITAM
ISP-020113	**Information Asset owner's security responsibilities**	
	Information asset owners must determine appropriate sensitivity classifications for information assets. Information asset owners must also make decisions about who will be permitted to access the information and the uses of this information. Information asset	Asset Owner

	owners must ensure appropriate handling is complied with.	
ISP-020114	**Information Asset custodian's security responsibilities**	
	Information asset custodians are responsible to define specific control (e.g. access control), implementation and maintenance measures, and provide recovery capabilities consistent with the instructions of information asset owner.	Information Asset Custodians, GIT
ISP-020115	**Information Asset user's security responsibilities**	
	All users of Gamuda Group' information assets must comply with the control requirements specified by the asset owner / asset custodian. Users may be employees, temporaries, consultants, contractors, or third parties with whom special arrangements have been made.	ALL
ISP-020116	**Authorization for information processing facilities**	
	The use of new information processing system (both hardware devices and software packages) or significant change of existing information processing system shall be authorized by Head of Global Infra.	Head of Global Infra
Objective: Outsourcing and Third Party Contracts		
Description	To maintain the security of Gamuda Group information processing facilities and assets accessed by third parties or outsourcing vendors. Maintain the security of information when the responsibility for information processing has been outsourced to another organization.	
ISP-020201	**Security Requirements in Outsourcing and Third Party Contracts**	
	The security requirements of Gamuda Group outsourcing the management and control for all or some of information system, networks and/or desktop environments, or other activities must be addressed in a contract agreed between the parties. The person in charge need to consider the minimum-security criteria.	Project Owner, GIT, ITGC, Cybersecurity
ISP-020202	**Non-Disclosure Agreements**	
	Employees must not disclose sensitive information to consultants, contractors, or third parties before receipt of a signed non-disclosure agreement.	ALL

ISP-020203	**Handling Risks Associated with Outsourcing of Information Services**	
	The contract for outsourcing arrangements must adhere to Gamuda Group Information Security Policy.	ALL
ISP-020204	**Return of Gamuda Group Information Assets**	
	All Gamuda assets must be returned upon completion of work and adhere to Information Security Policy.	ITAM

DOMAIN 03 - INFORMATION & PROCESSING DEVICES ASSET MANAGEMENT		
Objective: Accountability for Information Assets		
Description	To maintain appropriate protection of organizational information assets.	
ISP-030101	**Inventory of Information & processing devices assets**	
	An inventory of information assets in Gamuda Group is using IT inventory system.	ITAM
ISP-030102	**Categories of IS assets**	
	Inventory of IT assets in Gamuda Group consist of: 1. *Data and information* 2. *People* 3. *Software* 4. *Hardware/physical* 5. *Services*	ITAM
Objective: Information Classification and Handling		
Description	To ensure that information assets receive an appropriate level of protection.	
ISP-030201	**Information classification scheme**	
	The information asset is classified to indicate the need, priorities and degree of protection. The asset owner is required to define the classification of information during its creation. These classifications are defined as: 1. Confidential. 2. Restricted. 3. Internal Use. 4. Public Information.	ALL

ISP-030202	**Information labelling**	
	All information must be labelled with an appropriate data classification according to the classification scheme. Such markings must appear at all manifestations of documented information (digitised or hardcopy).	ALL
ISP-030203	**Third party interactions**	
	Unless it has specifically been designated as **Public Information,** or intended for public use, all internal information must be protected from disclosure to third parties. Third parties may be given access to Gamuda Group internal information only when a demonstration of a need-to-know basis exists.	ALL
ISP-030204	**Prior review**	
	Every speech, presentation, technical paper, book, or other communications to be delivered to the public media must first be approved for release by the Group Corporate Communications Department (GCC).	ALL, GCC
ISP-030205	**Information handling**	
	All the following types of information processing activity: 1. Copying 2. Storage. 3. Transmission by spoken word, post, fax and electronic mail. 4. Destruction Shall adhere to the handling specified in Information Handling Procedure	ALL
ISP-030206	**Information Retention & Reuse**	
	All information that is classified Confidential, Restricted and Internal Use regardless the medium shall be deposited and stored into the approved storage location. The reuse of inactive information and records shall be controlled. The preservation, storage and retrieval should comply to international standard and best practice.	ALL

DOMAIN 04 - INFORMATION SECURITY RELATED TO HUMAN RESOURCE		
Objective: Training Awareness		
Description	To reduce the risks of human error, theft, fraud or misuse of facilities.	
ISP-040101	**Information security training**	
	All employees must be provided with adequate awareness & training to allow them to properly protect/use Gamuda Group information resources. New employees must be briefed and made aware of their security obligations.	GIT Training and Recruitment Unit
ISP-040102	**Information security awareness**	
	Awareness initiatives need to be conducted regularly as part of an annual program to remind employees about their obligations with respect to information security.	GIT Training and Recruitment Unit
ISP-040103	**Compliant to ISP and Procedures**	
	Every employee must understand and comply to Gamuda Group ISP. Failure to do so will be subjected to disciplinary action.	ALL, HR
ISP-040104	**Security in job responsibilities**	
	Every employee shall be responsible to preserve the confidentiality, integrity and availability of Gamuda Group information asset and data.	HOD, HR
Objective: Human Resources Matter		
Description	To ensure the personnel are aware of information security threats and concerns and are equipped to support organizational security Policy in the course of the normal work.	
ISP-040201	**Disciplinary action for Information Security Policy non-compliance**	
	Non-compliance with ISP, standards, or procedures is grounds for domestic enquiries that can result in disciplinary actions up to termination of employment and legal actions.	ALL, HR

ISP-040202	**Employee screening**	
	Basic verification checks on all newly recruited employees must be carried out at the time of successful employment with Gamuda Group.	HR
ISP-040203	**Action in response to employee termination**	
	In the event that Gamuda Group employee is terminating his or her relationship with Gamuda Group, the HOD must inform the HR immediately.	HOD, HR, Business Unit
ISP-040204	**Compliance to ISP**	
	All employees must adhere to the ISP at the time they join the company.	HR

DOMAIN 05 - INFORMATION SECURITY RELATED TO PHYSICAL & ENVIRONMENTAL		
Objective: Building Access Control		
Description	To prevent unauthorized access, damage and interference to business premises and information.	
ISP-050101	**Physical access control for secured areas**	
	Access to Data Centre, Command Centre, Security Operation and areas containing information labelled as Confidential and Restricted or critical infrastructure must be physically restricted. Only the facility owner authorized to grant physical access to these premises. Record of granted access shall be retained by respective department. Access to restricted areas within Gamuda Group premise during off-office hours, weekends, and public holidays shall be controlled. All access shall adhere to the zoning system identified. All entrance the centre must be installed with door access system. Locations with 24 hours man surveillance are exempted with door card access. Access from emergency exit to computer facilities in the centre from outside must be prevented.	ALL, HR, GIT

ISP-050102	**Physical access control log**	
	Each person shall present his/her Gamuda Group issued identification card, or be constantly accompanied by as staff member, before entering every controlled door or area within Gamuda Group premises. The party who authorized the access shall maintain the physical access log. Access logs that shall be maintained are: 1. Access card system 2. Third party access to Confidential and Restricted information area and critical infrastructure area 3. CCTV logs Admin department will initiate review of physical access log records with respective information asset owners.	ALL, ADMIN
ISP-050103	**Reporting lost or stolen Identification Badges**	
	The return notice and instruction must be made visible on all identification badges. Identification badges that are lost or stolen must be reported immediately by the employee to the appropriate party who issues the card (i.e. HR). The Project Owner concern share the responsibility on the lost of identification badge by employee or third party.	HR
Objective: Building Access Control		
Description	To prevent unauthorized access, damage and interference to business premises and information.	
ISP-050201	**Working in secured areas**	
	While working in secured areas, the following controls should be observed to enhance the security of a secured area: 1. Unmanned secured areas must be physically secured and periodically checked. 2. Third party support services personnel is granted restricted access to secured areas	ADMIN

	only when required. This access must be authorized and monitored. Drone, photographic, video, audio or other recording equipment shall not be allowed to be used, unless authorized by the facility owner.	Group Corporate Communication.
ISP-050202	**Working in secured areas after official business hours**	
	If access to Gamuda Group facility has been restricted because sensitive, critical, or valuable information is handled therein, working in secured areas by employee or third parties after normal working hours is only permissible upon authorization from facility owner.	ALL,GIT
ISP-050203	**Unobtrusive site (for secured areas)**	
	Buildings or rooms that are designated as secure areas should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside the area identifying the presence of information processing activities.	INFRA, EUSS, ITAM
ISP-050204	**Isolated delivery and loading areas (for secured areas)**	
	Delivery and loading areas should be controlled and isolated from secured areas to avoid unauthorized access. Third parties need to register at the Security Guard and load the items at the designated areas and have them delivered to relevant parties with proper sign-off.	GIT, ADMIN
Objective: Handling Visitors		
Description	To prevent compromise or theft of information and information processing facilities.	
ISP-050301	**Identification and sign-in process required for all visitors**	
	All visitors accessing the secured areas must be logged. Visitors must be admitted to Gamuda Group premises only for specific authorized purposes.	ALL

ISP-050302	**Supervised third party access**	
	Visitors (e.g. customers, contractors) must be escorted to secure areas by Gamuda Group employee.	GIT
ISP-050303	**Individuals seen without identification badges must be questioned**	
	Individuals seen by Gamuda Group staff without a proper Gamuda Group identification badge (or badge that is not put on a visible place) must be immediately questioned. If the visitor cannot promptly produce a valid badge, they must be escorted to the Security or receptionist.	ALL
Objective: Hardware, Peripheral and Other Equipment Security		
Description	To have better guidance in handling physical equipment.	
ISP-050401	**Preparing premises to site information processing equipment**	
	The sites chosen to locate information processing equipment and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards. All production servers servicing customers must be housed in the Data Centre.	INFRA
ISP-050402	**Fire, water and physical intrusion alarm trigger immediate action**	
	Gamuda Group Data Centre & Disaster Recovery Site must be equipped with fire and physical intrusion alarm system that automatically alert those who can take immediate action. Installation of fire detection system, if any, must comply with local regulations. Fire detection system must be checked to ensure that these have been suitably installed, and must be regularly checked and serviced, at least on an annual basis. Smoking, eating and drinking must be strictly prohibited in the Data Centre.	GIT

	Equipment, paper and flammable materials not essential to the operations must NOT be stored in the Data Centre.	
ISP-050403	**Power supplies**	
	To ensure the continuity of services, all critical equipment in Gamuda Group offices must use surge suppressors. Core systems must be connected to UPS’s and a generator set.	GIT, ADMIN
ISP-050404	**Security equipment off-premises**	
	Any use of equipment for information processing outside Gamuda Group premises must require authorization by the facility owner. Log of equipment movement and usage shall be maintained.	INFRA
ISP-050405	**Disposal and reuse of IT equipment**	
	Confidential and Restricted information must be erased, where applicable from equipment or overwritten (reformat) prior to disposal or re-use. The authorization to dispose equipment must be obtained from IT Asset Management. All equipment that have been classified as beyond repair that can no longer be used or have been replaced with new equipment should be sent back to GIT for disposal and write-off. The respective department should only prepare the transfer of the equipment to GIT for onwards write-off or disposal. The equipment should not be retained by the users as further use of the equipment constitutes an illegal use of software.	ITAM, EUSS
ISP-050406	**Clear desk and screen**	
	A clean desk and screen can be an important tool to ensure that all confidential and sensitive materials are removed from user workspace and locked away when the items are not in use or user leaves his/her workstation. It is one the strategies in reducing the risk of security breaches in the workplace. This can also increase user’s awareness about protection of sensitive information.	ALL

	▪ Users are required to ensure that all confidential and sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and whenever they are away from their work area. ▪ Computer workstations must be locked when workspace is unoccupied. ▪ Computer workstations must be shut completely down at the end of the work day. ▪ File cabinets containing confidential and sensitive type of information must be kept closed and locked when not in use or when not attended. ▪ Keys used for access to confidential and sensitive type of information must not be left at an unattended desk and cabinets. ▪ Notebook and mobile devices must be either locked with a locking cable or locked away in a drawer. ▪ Passwords may not be left on sticky notes posted on or under a computer, not may they be left written down in an accessible location. ▪ Printouts containing confidential and sensitive type of information should be immediately removed from the printer. ▪ Upon disposal confidential and sensitive type of documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins. ▪ Whiteboards containing confidential and sensitive information should be erased. ▪ Treat mass storage devices such as CDROM, DVD, USB drives and External Hard Disk as sensitive and secure them in a locked drawer.	
ISP-050407	**Removal of property**	
	Equipment, information or software belonging to Gamuda Group must not be removed (i.e. transferred, deleted) without authorization of the IT Asset Management.	ITAM

ISP-050408	**Loss of equipment**	
	Every user is responsible and accountable for the desktop computer, notebook, accessories and licences that have been assigned to them. Users are to ensure against any tempering, missing, stolen or loss of equipment. Users are to make police report for any loss items and report to IT Asset Management for record purposes. Insurance section should be immediately informed for insurance claims (if any).	ITAM, Megah Management Services (insurance), HR
ISP-050409	**Cabling security**	
	Network cabling must be protected from unauthorized interception or damage. The cables within the data centers must be labeled accordingly.	GIT
ISP-050410	**Equipment maintenance at Data Centre**	
	Electrical system and distribution box within the Data Centre is checked at least annually. All equipment housed in the Data Centre that belongs to Gamuda Group.	GIT
ISP-050411	**Faulty IT Equipment**	
	Equipment under GIT Ownership which needs to be repaired will be sent to the appropriate vendors for repair. GIT or the vendor shall provide a replacement unit – subject to availability of spare unit. Only authorised GIT staff shall liaise with the vendor for repair. GIT will maintain a log of all GIT equipment sent for repair and will follow-up very closely with the vendor to minimise any delay in repair. Only GIT shall determine whether faulty equipment is beyond repair. Users will be advised if the equipment cannot be repaired and to request for new equipment as replacement. For equipment that is faulty due to user carelessness or negligence, the cost of repair may be charged back to the user unless the user can prove otherwise.	ITAM, EUSS, INFRA
ISP-050412	**The use of Desktop Computer**	
	• Desktop computers are provided exclusively for the use by staff in accordance with their normal duties of employment. All other use is private. Private use is allowed, as a privilege and not a	ALL

	right, but if abused will be treated as a breach of the employment regulations. • The devices, software & hardware accessories, components, and programs, which belong to the company shall be preserved and protected at all time. • Only authorised workstations can access to Gamuda Group network, company information and business applications. • It is not permitted to download any software applications, programs, executable files by any users. Only authorised IT technical support staff can perform the necessary download. • Software on PCs will also be regularly reviewed as part of PC maintenance and replacement. • Users shall be fully responsible and accountable for the materials, contents, outputs and files on the computer devices as well as the integrity of data stored on the devices and its accessories. All official data related to the business of the company should be stored in the shared location accessible to the respective group as setup by GIT. • Users will be held personally responsible for any problems caused by their negligence.	
ISP-050413	**The use of Notebook & Mobile Devices**	
	• Notebook and mobile devices are provided exclusively for the use by staff in accordance with their normal duties of employment. • All notebooks, mobile devices and its accessories are the property of Gamuda Group and are provided to staff for a period of time as deemed appropriate. • Only authorised workstation/devices by GIT can access to Gamuda network, company information and business applications. • Users must NOT install software or hardware or change the system configuration including network settings without prior consultation with GIT.	ALL

	• Users must protect company's workstation and devices from damage and theft. Safety and security of workstations and devices shall be given utmost importance. • Users will be held personally responsible for any problems caused by their negligence. • It is not permitted to download any software applications, programs, executable files by any users. Only authorised GIT technical support staff can perform the necessary download. • Workstations and devices must not be loaned to any authorised personnel, friends, family members etc. • Users shall be responsible to the intellectual property rights and ensure the use of licensed software only. • Users shall not make changes or do anything on the workstations and devices or its accessories such that it may adversely affect the performance of the device or make it exposed to viruses.	
ISP-050414	**The use of Printer**	
	i) Print only those documents, which are relevant to the work, and related to the company. Excessive printing of personal documents is prohibited. ii) Standalone printers shall only be installed for those with specific business need as determined by GIT. iii) Make efforts to limit paper usage.	ALL, ITAM
ISP-050415	**The use of Your Own Device (BYOD)**	
	Bring Your Own Device or BYOD refers to privately owned devices (computing equipment, communication devices, storage devices, copying devices) used by Gamuda Group employees, suppliers and parties with Gamuda Group services to process, channel or access Gamuda Group networks, data, information and applications. BYOD users who have access to Gamuda Group information are subject to Information Security Policy.	ALL

DOMAIN 06 - INFORMATION SECURITY OPERATIONS MANAGEMENT & IT NETWORK		
Objective: Operational Procedures and Responsibilities		
Description	To ensure the correct and secure operation of information processing facilities.	
ISP-060101	**Formal change control procedure required for all live systems**	
	All computer and communications systems used for live processing at Gamuda Group shall employ a formal change control. For situation that involves change due to regulatory requirement, management directive, business process that affecting the information flow and service, the change management process should follow departmental change management process.	GIT
ISP-060102	**Change Management review/approval**	
	The change requestor must submit the request to be reviewed/approved by relevant HOD in the Service desk system.	ALL, GIT
ISP-060103	**Post-Change Management implementation review**	
	As part of the overall performance management and validation process, a review shall be warranted. The review for major changes is performed within 6 months after completion.	GIT
ISP-060104	**Segregation of duty**	
	It is at the responsibility of HOD to ensure segregation of duty subject to the sensitivity of the duties. Sensitive duties must be segregated to avoid collusion. Else, other controls such as monitoring of activities, audit trails and management supervision shall be considered. Logical access controls must be used to enforce segregation of duties between incompatible functions.	ALL,GIT,HR
ISP-060105	**Documented operational procedures**	
	All operating procedures must be documented and maintained, with changes being authorized by the HOD	HOD, ITGC

	or another authorized party and deposited in the designated repository.	
Objective: Information System Planning and Acceptance		
Description	To minimize the risk of system failures.	
ISP-060201	**Information processing capacity planning**	
	Capacity demands shall be monitored, and projections of future capacity requirements made to ensure that adequate processing power and storage are available. Asset Owner should work closely with GIT to determine the capacity requirements.	INFRA, ITAM
ISP-060202	**System acceptance**	
	Acceptance criteria for new information system, upgrades and new versions shall be established and suitable test of the system carried out prior to acceptance.	ALL, GIT
Objective: Protection Against Malicious and Mobile Code		
Description	To protect the integrity of software and information from damage by malicious software.	
ISP-060301	**Installing and maintaining of Endpoint Detection and Response (EDR)**	
	GIT will provide centralized security and continuously monitor threat of all end points of the network, delivering a comprehensive and holistic protection.	GIT
ISP-060302	**User responsibility in mitigating computer virus**	
	i) Security is every user's responsibility. Hence users are expected to be aware of the security threats like virus attacks, hacking, trojan horses, worms, zombies, spoofing, phishing, spyware, adware etc. that may impact their valuable data stored in their respective workstation. ii) If the workstation or devices is suspected to be infected with virus, a message is received stating that a virus has been located in the workstation or devices, immediately send to GIT.	All

	iii) Most viruses arrive by email and many are spread by subscriptions to mailing lists. Therefore, only subscribe to work related mailing lists. iv) It is illegal to use the network services or equipment to develop or distribute any form of virus, trojan or any other form of malicious code. v) It is illegal to use the network services or equipment to attempt to hack or gain unauthorized access to any computer system. vi) Check out any suspicious or unexpected emails with the GIT team before opening them.	
ISP-060303	**Usage authorization of software**	
	All usage of software should be in compliance with software license and authorized by GIT.	ALL, GIT
ISP-060304	**Installation of Non-Standard Software and Hardware**	
	IT Asset Management will approve all non-standard software and hardware.	ITAM, EUSS, INFRA
ISP-060305	**Obtaining files and software**	
	Employees are prohibited to download any files and software from unknown sources (either from external network or any other medium) unless it has been scanned for malicious software before use.	ALL
Objective: Housekeeping		
Description	To maintain the integrity and availability of information processing and communication services.	
ISP-060401	**Data Storage**	
	▪ All data residing on the company issued workstation or devices are the property of Gamuda Group. ▪ Sensitive and mission critical data should NOT be stored on local devices. ▪ Data stored on the local device of workstation or devices is the sole responsibility of the user. ▪ Users are responsible for the safety, integrity, backup and recovery of any data stored on local drives of their workstation or devices.	ALL, GIT

	▪ GIT is NOT responsible for backing up/restoring of data kept on the local drive. ▪ All official data should be stored in the shared location accessible to the respective group as per business requirement so that data availability and integrity is maintained. Avoid keeping any personal data in shared location.	
ISP-060402	**Information back-up**	
	Back-up copies of essential business information and software for critical systems shall be taken regularly. The backup processes must be performed at least weekly or at a suitable frequency defined.	GIT
ISP-060403	**Off-site storage of back-up media**	
	All critical information/software recorded on back-up computer media must be stored in a different building.	GIT
ISP-060404	**Cloud Storage (Online Data Storage)**	
	GIT has provided the facility of One Drive as Gamuda Group cloud storage. As such, users are encouraged to utilise this facility as an online data storage and for sharing information.	ALL, GIT
ISP-060405	**Minimum information retention period**	
	Minimum information retention period is subject to criticality of data. Financial record shall be retain for 7 years while others must be kept for minimum 3 years or stipulated by regulation.	GIT
ISP-060406	**Logs required on application system handling sensitive information or task**	
	Business application systems or tasks, which handle sensitive information (Confidential and Restricted), must be able to generate transactional logs that show every addition, modification and deletion to such sensitive information.	SAP
ISP-060407	**Retention period of logs**	
	All critical application and system logs must be retained for future reference. As a minimum all logs must be kept for 12 months.	GIT

ISP-060408	**Logs Access Control**	
	All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. The GIT is the division responsible in defining the log access control and the owner of the information; while GIT is the custodian.	GIT
ISP-060409	**Amendments to System File**	
	All amendments to system files must only be made by GIT personnel. Users are prohibited to make any system file changes.	GIT
ISP-060410	**Back-up Responsibility**	
	Infra personnel are responsible to ensure that the back up is executed and adequate.	INFRA
ISP-060411	**Preservation of Cloud Service Security**	
	When Gamuda Group should only acquire service from established service provide.	GIT
Objective: Media Handling and Security		
Description	To prevent damage to assets and interruptions to business activities, media should be controlled and physically protected.	
ISP-060501	**Security of system documentation**	
	System documentation (i.e. operating manual, user manual, maintenance manual, etc.) must be stored securely and the access for the document should be kept to a minimum.	GIT
ISP-060502	**Handling of removable media**	
	The use of removal media shall be controlled within Gamuda Group. Removable media drives should only be enabled if there is a business reason for doing so.	GIT
ISP-060503	**Portable Memory & External Hard Drive**	
	▪ External hard drives and portable memory MUST NOT be used for long-term storage of Gamuda Group business data. ▪ External hard drives and portable memory devices are for temporary data storage only and may be used only to transfer/transport business data. Data	ALL

	MUST be deleted after transfer/transport business data. ▪ The use of external hard drive is allowed for the purpose of data backup if there is no other data backup facility available. ▪ Users using portable storage devices, and flash memory and external hard drive MUST ensure that such devices are free from virus and malware prior to use. ▪ Users must take every precaution to ensure the privacy of information on such devices.	
Objective: Media Handling and Security		
Description	To prevent damage to assets and interruptions to business activities, media should be controlled and physically protected.	
ISP-060601	**Information exchange agreements**	
	Agreements should be established for the exchange of information (whether electronic or manual) between organizations based on the sensitivity of the business information involved.	ALL
ISP-060602	**Security of media in transit**	
	All sensitive media in transit (e.g. via postal or courier) should be suitably protected.	ALL
ISP-060603	**Online Data security**	
	Where data or information is involved via online, Gamuda Group shall take security into considerations upon advice from GIT. Information involved in on-line transaction must be protected to prevent unauthorized disclosure.	ALL
Objective: Electronic Mail & Electronic Office System Security		
Description	To ensure the safeguarding of information in electronic and the protection of the supporting infrastructure.	
ISP-060701	**General use and ownership of email and office system**	
	While Gamuda Group desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the	ALL

	property of Gamuda Group. Because of the need to protect Gamuda Group network, management cannot guarantee the confidentiality of information stored on any network device belonging to Gamuda Group. For security and network maintenance purposes, authorized individuals within GIT may monitor equipment, systems and network traffic at any time. Gamuda Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.	
ISP-060702	**Email Authorized Use**	
	Data Protection Email messages are confidential to an individual. All emails will be monitored by GIT. **Distribution** Except for company related information that requires internal circulation, users should refrain from sending or forwarding emails such as greetings to a large group of people as this takes up a lot of resources. **Attachment** Attachments must be sent with care. Large attachment must only be sent to those who really require them. The email system commonly duplicates the attachment as many times as the number of recipients of the message. This takes a lot of disk space, thus impacting on performance and delivery of other messages. GIT encourage the use of One Drive facility in order to share documents instead of sending attachments.	ALL
ISP-060703	**Internet Authorized Use**	
	Use of Internet Gamuda Group recognises that the internet is an integral part of doing business and therefore encourages staff to use the internet whenever such use supports the company's goals and objectives.	ALL

	Gamuda Group also recognises that the internet is embedded in people's daily lives. As such, staff are allowed to use the internet for personal reasons at the company's discretion and in compliance with ISP.	
ISP-060704	**No Default protection**	
	Gamuda Group electronic mail system is not encrypted by default. Employee is not allowed to send confidential information unless it has been first encrypted or properly protected.	ALL
ISP-060705	**Scanning of attachments**	
	Employees need to ensure that attachments are scanned prior to download/open. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.	ALL
ISP-060706	**Message disclaimer**	
	A disclaimer encouraged be placed on all email messages.	ALL
ISP-060707	**Social Media**	
	Social media broadly include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletter, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner. All Gamuda employees shall adhere to Gamuda Social Media Policy by Group Corporate Communication.	ALL, GCC
Objective: Electronic Mail & Electronic Office System Security		
Description	To ensure the safeguarding of information in electronic and the protection of the supporting infrastructure.	
ISP-060801	**Audit Logging for System Logs**	
	Audit logs produced must record user activities, exceptions and information security events. The logs must be kept for a minimum 1 years to assist in future investigations and access control management.	GIT

ISP-060802	**Monitoring System Use**	
	Reporting for use of information processing facilities must be established. The results of the monitoring activities are to be reviewed and reported based on incident(s).	GIT
ISP-060803	**Protection of Log Information**	
	Logging facilities and log information should be protected against tampering and unauthorized access. If the logs reside on internet-accessible computers, which are not directly Internet-accessible.	GIT
ISP-060804	**Administrator and Operator Logs**	
	System administrator and system operator activities must be logged. These logs must be reviewed on a regular basis by Infra and SAP Basis Team.	INFRA
ISP-060805	**Fault Logging**	
	Faults reported by users or system programs related to problems with information processing or communications system shall be logged and analysed by EUSS. Appropriate actions must be taken.	EUSS, Cybersecurity, Infra
ISP-060806	**Clock synchronization for accurate logging of events on network**	
	All critical servers connected to Gamuda Group internal network shall always have the current time accurately reflected in their internal clock referenced to a recognized time-source.	INFRA

DOMAIN 07 - INFORMATION SYSTEMS ACCESS CONTROL		
Objective: Business Requirement for Access Control		
Description	To control access to information.	
ISP-070101	**When to use computer system access control**	
	All computer-resident information that is (confidential and above) sensitive, critical, or valuable must have system access controls to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable.	ALL

ISP-070102	**Disclaimer of responsibilities for damage to data and programs**	
	Gamuda Group uses access controls and other security measures to protect the confidentiality, integrity and availability of the information handled by computers and communications system. In keeping with these objectives, management maintains the authority to: 1. Restrict or revoke any user's privileges, 2. Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and 3. Take any other steps deemed necessary to manage and protect its information system. This authority may be exercised with or without notice to the involved users. Gamuda Group disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.	ALL
Objective: User Access Management		
Description	To ensure that access rights to information system are appropriately authorized, allocated and maintained.	
ISP-070201	**Allocation of privileges**	
	The privileges associated with each business application system, (e.g. operating system, database management system and each application) and the categories of employee to which they need to be allocated should be identified and authorized by the Asset Owner and implemented by GIT. Creation, amendment and maintenance of user and resource profiles can only be executed by GIT with written authorization from the Business Unit, which must be retained for validation. When authorizing access, the Asset Owner should consider the following. 1. Compatibility with other responsibilities and existing access rights of the user. 2. The classification of the information.	Asset Owner, GIT

	3. Whether the requested level of access is required in order to allow the user to carry out his/her normal duties. 4. Duration that access required, if access is needed on a temporary basis.	
ISP-070202	**Privilege restriction based on the need-to-know**	
	The computer and communications system privileges of all users, systems and programs must be restricted based on the need-to-know, i.e. the minimum requirement for their functional role only when needed.	GIT
ISP-070203	**Periodic review and reauthorization of user access privileges**	
	The system privileges granted to every user must be re-evaluated by the Business Unit and GIT at least annually for critical systems. This re-evaluation involves a determination whether currently enabled system privileges are still needed to perform the user's current job duties.	Business Unit, GIT
ISP-070204	**Information system access privilege terminated when employee leaves**	
	All Gamuda Group information system privileges must be promptly terminated or suspended at the time that employee ceases to provide services to Gamuda Group. ID's are also revoked if: 1. Misconduct of user that may interfere with normal and proper operations, or 2. Disturb others' use of information system Note: Controlled ID's such as root, administrator are exceptions to this requirement and follow other control procedures.	Business Unit, HR, GIT
ISP-070205	**Granting of user-ID and access rights to outsiders**	
	Individuals who are not employees must NOT be granted a user-ID or otherwise be given privileges to use Gamuda Group computers or communications system unless approval from the Business Unit and GIT has first been obtained. Before any third party is given access to Gamuda Group system and information, a formal agreement defining the terms and conditions of such access must	Business Unit, GIT, Cybersecurity

	have been signed by an authorized representative at the third-party organization.	
Objective: Network Access Control		
Description	Protection of networked services.	
ISP-070401	**Internal network addresses must not be publicly release**	
	The internal system addresses, configurations and related system design information for Gamuda Group networked computer system must be restricted such that both system and users outside Gamuda Group internal network cannot access this information.	GIT
ISP-070402	**Large network must be divided into separate domain**	
	All large networks crossing Gamuda Group boundaries must have separately defined logical domains, each protected with suitable security perimeters and access control mechanisms.	GIT
ISP-070403	**Internet connected machines must have an intrusion detection system**	
	To allow Gamuda Group to promptly respond to attacks, all Internet-connected devices must be protected by suitable technological platform	GIT
ISP-070404	**Live servers, staging servers and external network connections require firewalls**	
	All in-bound external connections to Gamuda Group internal networks or multi-user computer system must pass through an additional access control point (i.e. firewall) before users can reach a login banner.	GIT
ISP-070405	**Firewalls must run on dedicated system**	
	All firewalls used to protect Gamuda Group internal network must run on separate dedicated system. These computers may not serve other purposes such as acting as web servers etc.	GIT
ISP-070406	**Firewall configuration change requires information security approval**	
	Firewall configuration rules and permissible service rules shall not be changed without proper authorization.	GIT

ISP-070407	**Direct network connection with outside organizations**	
	The establishment of a direct connection between Gamuda Group system and computers at external organizations, via the Internet or any other public network, is prohibited unless this connection has first been approved by GIT. The network connections should be secured using a secure tunnelling.	GIT
ISP-070408	**Security requirements for network-connected third-party system**	
	As a condition of gaining access to Gamuda Group computer network, every third party must secure its own connected system in a manner consistent with Gamuda Group requirements. It is advised that third parties get security assessments performed on their system before connecting to the system within Gamuda Group. Gamuda Group reserves the right to audit the security measures in effect on these connected system without prior warning. Gamuda Group also reserves the right to immediately terminate network connections with all third party system not meeting such requirements.	GIT
ISP-070409	**Remote diagnostic port protection**	
	Access to diagnostic port should be securely controlled. The system administrator for a particular application system needs to work together with GIT (Network) to define ports that need to be opened.	GIT
ISP-070410	**User authentication for external connections**	
	Access by remote users to Gamuda Group network should be subject to authentication except those designated publicly accessible servers, e.g. public web servers, etc. Approval GIT is needed prior to authorizing remote access.	GIT
ISP-070411	**Wireless Policy**	
	GIT shall establish and ensure the appropriate protection of Gamuda Group data communication over wireless forms of transmission and reception.	GIT

ISP-070412	**Allowable Wireless Devices**	
	All wireless devices connected to Gamuda Group enterprise network must be certified by a certification agency prior to installation and use for processing business information. Where permissible, wireless devices encouraged be registered with GIT for inventory and audit purposes.	GIT
ISP-070413	**Deployment of Wireless Communications Devices**	
	Wireless deployments should conform to existing Gamuda Group administrative and operational procedures. Wireless network deployment should comply with overall organization network architecture and security requirements. Wireless devices are placed in separate network and intrusion detection system is used to monitor the network traffic. Wireless network deployment should take into account physical security issues surrounding wireless enabled workstations and system, location of wireless access points and access control to physical media, system and facilities. This control represents practices and procedures to protect physical devices from unauthorized access or exploitation. Default wireless setting must be changed prior to deployment and it should not contain any identifying information about the organization information or vendor product identifier. Passwords required to access wireless devices console should comply with organization password policies. GIT should ensure that anti-virus software is installed and configured in accordance with the company personal computer practice on all wireless connected devices, and kept up-to-date with most recent virus definition tables.	GIT
ISP-070414	**Access Control on Wireless Communications**	
	Wireless access should implement user-based access control by requiring user to authenticate prior gaining access to the wireless network. This control may include authentication password at the wireless access-points. Each user is required to have an	GIT

	assigned IP address before wireless access is provided.	
ISP-070415	**Encryption on Wireless Communications**	
	To ensure the data confidentiality, authentication and integrity, wireless devices must use highest and recommended encryption available. All implementations must support hardware address that can be registered, tracked and firmware updated. Existing hardware that does not support current security standard and features should be upgraded and/or replaced.	GIT
Objective: Operating System Access Control		
Description	To prevent unauthorized computer access.	
ISP-070501	**Before log-on**	
	It is encouraged to have a general notice warning that the computer should only be accessed by authorized users should be displayed on critical system.	GIT
ISP-070502	**Limit on consecutive unsuccessful attempts to log-on**	
	To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited.	GIT
ISP-070503	**Upon successful log-on**	
	On completion of a successful log-on, the following information should be displayed to critical system: 1. Date and time of the previous successful log-on, or 2. Details of any unsuccessful log-on attempts since the last successful log-on (log).	GIT
ISP-070504	**Unique user-ID and password required**	
	All users (including technical support employee, operators, network administrators, etc) must have a unique identifier (user-ID) and password for their personal and sole use so that activities can subsequently be traced to the responsible individual.	ALL

	Please note the user-ID and password must be unique per user, not necessarily per system.	
ISP-070505	**Access to Users' Desktop and Notebook**	
	IT technical personnel shall have the right to access users' desktop computer and notebook (with prior notice) during non-office hours or via remote connect for troubleshooting, maintenance and software installation purposes.	GIT
ISP-070506	**Multiple Sessions**	
	The simultaneous log-on at two (2) or more terminals, system or application using the same user-ID is only allowed for identified system.	GIT
ISP-070507	**Minimum password length**	
	The minimum password length is to follow the User Access Management Procedure.	ALL
ISP-070508	**Quality password**	
	The quality of password is to follow the User Access Management Procedure.	ALL
ISP-070509	**Periodic password change**	
	The periodic password change is to follow the User Access Management procedure	GIT
ISP-070510	**Removal of unnecessary system software at installation time**	
	All system software which will definitively not be used at the present time and which comes along with the operating system or other system software should be removed from production system at the time when the operating system or other system software is installed.	GIT
ISP-070511	**Desktop Computer Upgrade**	
	Desktop computer upgrade happens when an existing desktop computer is replaced with a new desktop computer but without having to purchase new software license. All applicable licenses will be transferred from old desktop computer to the new desktop computer. As such, upon desktop computer upgrade, the old desktop computer can no longer be used as it no longer has a valid software license. The old desktop computer needs to be returned to IT as soon as the new desktop	GIT

	computer is delivered to avoid any breach of illegal software usage.	
Objective: Application Access Control		
Description	To prevent unauthorized access to information held in information system.	
ISP-070601	**Before log-on**	
	Users of applications system should be provided with access to information and application system functions in accordance with a defined access control procedure.	GIT
ISP-070602	**Limit on consecutive unsuccessful attempts to log-on**	
	All Gamuda Group staff user-ID / passwords privileges for live Gamuda Group business application system must be created and managed centrally through the GIT.	GIT
Objective: Mobile Computing & Telecommuting		
Description	To ensure information security when using mobile computing and teleworking facilities.	
ISP-070701	**Telecommuting privileges**	
	To refer to Remote Working Procedure.	HR
ISP-070702	**Mobile device used for corporate business information**	
	To refer to IT Asset Management Procedure.	ITAM

DOMAIN 08 - INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE		
Objective: Security in Application System		
Description	To ensure that IT projects and support activities are conducted in a secure manner.	
ISP-080101	**Security requirements analysis and specification**	
	All Project Owner must take security into consideration during the design stage of the application system (for both in-house and outsourced software development). GIT should be consulted on security. All software development efforts are to follow proven system	Project Owner, GIT

	development life cycle, where security measures are defined at every stage of the entire process. Risks must be analysed and countermeasures must be introduced.	
ISP-080102	**Correct processing of applications**	
	Appropriate controls and audit trails should be designed into application system. These should include the validation of input data, validation of output data, internal processing, authenticity and integrity of messages, etc.	Business Unit, Project Owner, GIT
Objective: Cryptographic Control		
Description	To protect the confidentiality, authenticity or integrity of information.	
ISP-080201	**Protection of encryption key**	
	Encryption is used for confidential and proprietary information and is defined as sensitive and/or critical and that is stored in non-secure locations or transmitted over open networks such as the Internet. The GIT are responsible for developing procedures for key management usage and for facilitating user training. Encryption keys should be protected with the most stringent security measures and must not be revealed to others. Any potential compromise of a secret key must be reported immediately to GIT.	GIT
ISP-080202	**Key Management**	
	All keys must be protected against modification, destruction, or unauthorized disclosure throughout the entire lifecycle of the key. To assure interoperability and consistency across the enterprise. The encryption standards ensure secure generation, storage, and transmission of keys as well as ensuring interoperability and key recovery (i.e. Management must be able to retrieve encryption-keys used for encrypted company information in storage)	GIT

Objective: Security of System Files		
Description	To ensure that IT projects and support activities are conducted in a secure manner.	
ISP-080301	**Updating of live business application software libraries and components**	
	The updating of the operational program libraries should only be performed by the nominated administrator (custodian).	GIT
ISP-080302	**Live Gamuda Group business application system must not store source code**	
	Live business application system must not store source code.	System Administrator, GIT
ISP-080303	**Audit log maintained for program update**	
	An audit log should be maintained for all updates to operational program libraries. Audit logs should be archived for One (1) years as minimum.	GIT
ISP-080304	**Previous versions of software retained**	
	Previous versions of software (one version behind UAT) should be retained as a contingency measure.	GIT
ISP-080305	**Access control in test environment**	
	The access control procedures, which apply to operational application system, should also apply to test application system. Test data, applications, and system must be protected accordingly from un-authorized access and modifications.	GIT
ISP-080306	**Deletion of information in test environment**	
	Operational (production) information should be erased from a test application system immediately after the testing is completed.	GIT
ISP-080307	**Technical review of operating system changes**	
	GIT should be sensitive to changes on operating system and install a newly supplied software release or patches. Patches or software release shall be validated prior to apply to live environment.	GIT, ALL

	OS update happens in regular frequencies. Users must not stop the OS update process while it runs in the machine.	
ISP-080308	**Restriction on changes to software packages**	
	Modifications to software packages must be strictly controlled and be approved by the management team. Changes must be fully tested and documented by GIT and approved by various parties involved prior to release.	GIT

DOMAIN 09 - INFORMATION SECURITY INCIDENT MANAGEMENT		
Objective: Reporting Information Security Events and Weaknesses		
Description	To ensure information security events and weaknesses associated with information system are communicated in a manner allowing timely corrective action to be taken.	
ISP-090101	**Reporting security events, malfunctions and weaknesses**	
	All security incidents (either real or suspected), malfunctions and weaknesses shall be reported as quickly as possible to the relevant parties. Incidents that may jeopardize the preservation of information confidentiality, integrity and availability shall be forwarded to the EUSS.	ALL, GIT
ISP-090102	**External reporting of security violations**	
	Information security violations that is notified to GIT will be reported to police.	GIT
Objective: Management of Information Security Incidents and Improvements		
Description	To ensure consistent and effective approach is applied to the management of information security incidents.	
ISP-090201	**Collecting evidence of security violations**	
	Evidence relating to a security incident must be properly collected and preserved for future investigation.	GIT

ISP-090202	**Investigating information security incidents and malfunctions**	
	All security incidents must be properly investigated and analyzed. GIT must respond accordingly to all incidents, liaising and coordinating with colleagues to both gather information and offer advice.	GIT
ISP-090203	**Corrective and preventive activity**	
	Counter measure shall be taken to recover from security incidents. Subsequently, corrective action must be taken to avoid the re-occurrence of the incident where appropriate.	GIT
ISP-090204	**Lesson learned from information security incident**	
	Where necessary, lesson learned from information security incident must be propagated to Gamuda Group employees to hinder similar instance from recurring and improvise delivery mechanism.	GIT, ITGC

DOMAIN 10 - INFORMATION SECURITY RELATED TO BUSINESS CONTINUITY MANAGEMENT		
Objective: Business Continuity Management		
Description	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.	
ISP-100101	**BCP Ownership**	
	Responsibility for developing and implementing processes to assess and provide Business Recovery and Incident Response requirements in the event of a loss of IT facilities & all department services must be formally identified. Business Recovery Planning and Incident Response Planning reviews must be completed for all critical system and services, in the course of which, risks should be identified, evaluated and all reasonable measures taken to reduce or eliminate threats.	ITGC (HR to initiate).
ISP-100102	**BCP Review and Maintenance**	
	The BCP must be reviewed and maintained periodically in response to any changes affecting the basis of the original business impact analysis and security risk assessment. The review is to be carried out as and	HR to initiate

	when required or every twelve (12) months, whichever is earlier.	
ISP-100103	**Assessing the Security Risk**	
	A risk assessment and business impact analysis is to be undertaken in order to determine the requirements of BCM. Frequency of above is at least annually, or as needed (when there are changes to the current system which impacted the recovery time or method; or, when new system are introduced).	HR to initiate
ISP-100104	**Training and Awareness Program on BCP**	
	All employees must be made aware of the BCP and their respective roles. The BC Coordinators is responsible in coordinating the training and awareness program on BCP every 12 months.	HR to initiate
ISP-100105	**Testing the IT BCP**	
	The DRP is to be re-tested once a year (or after major changes, whichever is sooner) in order to ensure that the employees know how it is executed. Other components of BCP are to be tested annually or after major changes, whichever is sooner.	BC Coordinators, DR Coordinators
ISP-100106	**Responsibility for BCM**	
	Employees are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts Gamuda Group business activity. It is the responsibility of each business unit to work closely with the BC Coordinators to develop, maintain, review and test plans for business continuity in the event of loss of any mission-critical facility and to train staff in the use of these plans.	ALL
ISP-100107	**Public Relations**	
	Employees are expected to maintain their discretion with respect to the disaster in the initial stages and to treat information regarding the disaster as confidential. External communications such as to news media, the general public, clients, and public authorities is the responsibility of the Corporate Communications Department.	ALL, GCC

ISP-100108	Storage and Distribution of BCM Documents	
	BCM documents with the complete procedures for response, recovery and resume must be readily accessible by BCM Committee and other teams that are involved in recovery and resumption processes. The BCP should be stored in a secure place (like Documentation Room/Cabinet) within the Gamuda Group premise. Another copy is stored in secure offsite storage. Each member of the BCM Committee and other teams that are involved in recovery and resumption processes, will also keep a copy of the relevant sections of the plan and it must be stored safely outside of the office e.g. in the car or another premise etc.	HR to initiate

DOMAIN 11 - INFORMATION SECURITY RELATED TO LEGAL & CONTRACTUAL COMPLIANCE		
Objective: Intellectual Property Rights		
Description	To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.	
ISP-110101	**Assignment of patent, copyright and other intellectual property rights**	
	While serving for Gamuda Group, all employees grant Gamuda Group the exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop for job related materials or tools.	ALL
ISP-110102	**Property rights to computer programs and documentations**	
	Without specific written exceptions, all programs and documentation generated by, or provided by employees, consultants, or contractors for the benefit of Gamuda Group are the property of Gamuda Group	ALL
ISP-110103	**Legal ownership of information system files and messages**	
	Gamuda Group has legal ownership of the contents of files stored on its computer and network system as well as all messages transmitted via these systems. Gamuda Group reserves the right to access this	ALL

	information without prior notice whenever there is a genuine business need.	
ISP-110104	**Attribution of sources for information**	
	Gamuda Group employees should always give proper credit to the source of information used for Gamuda Group purposes.	ALL
ISP-110105	**Relevant information security regulations, acts and standards**	
	Relevant Information Security regulations, acts, and standards to be complied to are listed below. ITGC is responsible in determining the requirements that are relevant to Gamuda Group within the below-listed documents. 1. Personal Data Protection Act 2010 2. Computer Crime Act 1997 3. ISO/IEC 27001 4. Copyright Act 1987 (with Amendment in 1997) 5. National Cyber Security Agency (NACSA), Majlis Keselamatan Negara.	ITGC
Objective: Protection of Intellectual Property Rights		
Description	To ensure compliance of system with organizational security policies and standards.	
ISP-110201	**Copyrights notices on computer programs and documentations**	
	All approved computer programs developed, owned by Gamuda Group and have been released and used in Gamuda Group' live business environment should include appropriate copyright notices. All approved manuals, guidelines and standards developed and owned by Gamuda Group should include appropriate copyright notices.	ALL
ISP-110202	**Periodic review of software/maintenance licensing agreements**	
	The agreements for all computer programs licensed from third parties should be reviewed on a need basis, by ITAM.	ITAM
ISP-110203	**Copying, transferring or disclosing of software prohibited**	
	Third party software in the possession of Gamuda Group must not be copied/transferred/disclosed unless	ALL

	such activity is consistent with relevant license agreements and either: 1. Management has previously approved of such copying, or 2. Copies are being made for contingency planning purposes. 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.	
ISP-110204	**Removal of unauthorized copyrighted information and software**	
	Third party copyrighted information or software, that Gamuda Group does not have specific approval to store and/or use, must not be stored on Gamuda Group system or networks. System administrators will remove such information and software unless authorization from the rightful owner(s) can be provided by the involved users. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Gamuda Group or the end user does not have an active license is strictly prohibited.	ALL, SA
ISP-110205	**Adherence to Intellectual Property Rights**	
	Gamuda Group strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Unauthorized copies of software are strictly forbidden by Gamuda Group. Likewise, Gamuda Group allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.	ALL
ISP-110206	**Use of Gamuda Group Information for Non-Business Purposes**	
	Gamuda Group information (product specifications, databases, mailing lists, internal software, computer documentation, etc.) may only be used for the business purposes specifically allowed by management. Use of these information resources for any other reason will be	ALL

	permitted only after written permission has been granted by the designated owner of the information.	
ISP-110207	**Communication of Gamuda Group Confidential and Restricted information**	
	Unless expressly authorized by owner of the documentation/information, sending, transmitting, or otherwise disseminating confidential and/or secret data (including and in particular trade secrets) of the company is strictly prohibited. Unauthorized dissemination of this information may result in internal disciplinary action.	ALL
Objective: Protection and Privacy of Personal Data		
Description	To ensure the privacy and protection of personal information	
ISP-110301	**Protection and privacy of Employee's personal use data**	
	While Gamuda Group desires to provide a reasonable level of privacy, employees should be aware that the personal use data they create on the corporate system remains the property of Gamuda Group. Because of the need to protect Gamuda Group network, management cannot guarantee the confidentiality of employee's personal use data stored on any device belonging to Gamuda Group	ALL
ISP-110302	**Right to Audit**	
	For security and network maintenance purposes, authorized individuals within Gamuda Group may monitor equipment, system and network traffic at any time. Likewise, Gamuda Group reserves the right to audit networks and system on a periodic basis to ensure compliance with this policy.	ALL
ISP-110303	**Privacy of Data for Web Users**	
	Gamuda Group is concerned about the way its business partners and itself handles private data of web users. The policy recognizes that information is one of the most valuable assets and issues the following privacy guidelines and recommendations to its business partner that deals with the applications supplied.	ALL

	Gamuda Group advocate a clear and fair privacy policy. Management must make reasonable efforts to ensure that all personal information is used only as intended, and that precautions preventing misuse are effective and appropriate.	
ISP-110304	**Disclosure of Information of Employees**	
	Disclosure of private information about the company's workers to third parties shall not take place unless: 1. Required by law or regulation, 2. Permitted by clear and explicit consent of the subject, or 3. After receipt of written commitment from third party organizations that information will be protected by adequate levels of security and privacy as determined by the Legal & Company Secretarial, and explicit consent is obtained from HRA.	ALL
Objective: Review of Information Security		
Description	To ensure compliance of system with organizational security policies and standards.	
ISP-110401	**Independent review of information security**	
	The ISMS Internal Audit must perform compliance checking related to information security Policy, standards and procedures annually. These reviews must include efforts to determine both the adequacy of and compliance with controls.	ITGC
ISP-110402	**Technical compliance checking**	
	Simulation or Penetration testing (to critical services and system) or services must be carried out annually or as needed to ensure compliance with security implementation standards. The testing must be performed by an independent party.	GIT
ISP-110403	**Legacy Hardware and System**	
	Obsolete or old hardware and system exposes vulnerabilities to Gamuda Group that attributed via product end of life; or product end of support; or decommission hardware and/or system. The	ITAM

consequence to this is no security updates from product principal; no technical support; and minimal or not possible to apply latest security control on emerging threat. As a result, malware can easily exploit unpatched vulnerabilities and quickly spread across Gamuda Group network. This may have adverse consequences and high financial cost implication and potential service disruption to Gamuda Group.

1. Product end of life is a product at the end of the lifecycle which is a retired from the market that involve pulling the product from the market without replacing it.

   Hardware and system administrators must aware and propose to Business Unit for new product or replace with a product with similar or better capability. It is strongly recommended not to have any new development or new investment in system and technology that is end of life.

   Should the hardware and or system still made available for use, administrators must ensure that product principal continue to provide post warranty support.

   Prior in getting the replacement for retired hardware or system, administrators shall apply short term mitigation to reduce the possibility of compromise by preventing access of untrusted content on vulnerable device.

   In case, if the hardware and system cannot be refresh, maintenance from product principal / OEM must be available in ensuring continuous confidentiality, integrity and availability. At the end of principal / OEM support, a third-party maintenance must be made available accordingly.

2. Product end of support is a product that is ending of services and updates for systems, servers, storage and network equipment. This situation prevents Gamuda Group from

receiving any updates and support from product principal.

Hardware and System administrators should initiate product end-of-support to be upgraded and replaced with pertinent release. High-risk end user devices and server should be prioritized for upgrades especially devices that can access to more sensitive information or services including personal data.

Hardware and system administrator is responsible to inform Business Unit on product end-of-support and work with them on the mitigation plans and activities in reducing risk for product end of support for hardware and/or system.

3. Decommission hardware and system is a situation where the hardware and/or system is retired and replaced by a new system covering the same functionality.

   Hardware and system administrator is responsible to isolate and disintegrate decommission hardware and system from the network and to power down from any access. Any need to access to decommission hardware and system must be approved by Business Unit and Head of GIT.

   In a situation where a decommission hardware and/or system is still made available to users to allow retrieval of old useful data continuously, the hardware and system must be configured on need-basis to the users with limited accessibility and minimal network connectivity.

Objective: System Audit		
Description	To maximize the effectiveness of and to minimize interference to/from the system audit process.	
ISP-110501	**System Audit Controls**	
	Audit requirements and activities involving operational system must be carefully planned and agreed to minimize disruptions to business processes. 1. Audit requirements should be agreed with ITGC. 2. The scope of the checks or audits should be agreed and controlled. 3. The checks or audits should be limited to read-only access to software and data. 4. Access to operational system (if applicable) other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed. GIT is to inform ITGC upon completion of the tasks for the removal of the affected files. 5. Resources for performing the audits or checks should be explicitly identified and made available. 6. Requirements for special or additional processing should be identified and agreed. 7. All access to audited system by any appointed auditors should be monitored at least by one system administrator and logged by GIT to produce a reference trail. 8. All audit procedures, scope, plan and responsibilities should be documented. 9. Access to system audit tools should be protected to prevent possible misuse or compromise.	GIT, ITGC