A. Background

Information Security policies are the foundation of information system security within a modern organization, and this document provides guidance to everyone in Telkomsigma, its not only limited to Managed Services (“MS”), and offers solutions to ensure that every individual in the organization has a clear and defined roadmap for ensuring information system security.

This document is a major step towards a comprehensive, consistent, and meaningful security conscious environment within the organization. It lays a solid foundation for the development and implementation of secure practices within MS. The policies themselves are not instructional or overly descriptive. They represent the rules, which must be adhered to by all employees of IT Operation services unit.

This document must be reviewed and tested for suitability, adequacy and effectiveness annually or if any significant change to organization.

All employees of IT Operation services team are expected to know these policies and be aware of the procedures involved in complying with them.

B. COMPLIANCE, EXCEPTIONS, AND ENFORCEMENT

Compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues, and protecting Telkomsigma's information. Any non-compliance with this or any other security policy that results in the compromise of Telkomsigma information confidentiality, integrity and/or availability may result in disciplinary action and possible prosecution under applicable laws. Telkomsigma must take every step necessary, including legal measures, to protect its assets.

Telkomsigma must also take the steps it deems reasonable to assess and audit compliance with the policy.This means that there must be no assumption of privacy when using Telkomsigma business tools and resources (Internet, email etc.). Records of activities can be created and reviewed to monitor for threats, violations and abuse.

Telkomsigma specifically reserves the right to restrict any user from accessing any system or information, including access to the Internet or e-mail facilities.

B.1.Exceptions

Exceptions to the Information Security Policy must only be granted if an appropriate business justification for the exception is approved by management and the person requesting the exception fully accepts the additional risk posed by the exception. To apply for an exception to the Information Security Policy, the requestor must prepare a written request for the exception, along with a business justification, and submit the request for consideration.

Telkomsigma must maintain detailed records of any exception request, and it's status, for review. All exceptions to policy granted must be subject to regular review by Telkomsigma and original sponsor for continued requirements. Any condition determined to be no longer required must be terminated with appropriate documentation filed for future review.

B.2. Enforcement and Violation Handling

Any compromise or suspected compromise of this policy must be reported to the appropriate management and Telkomsigma. All violations of security policies and/or standards are subject to disciplinary action by company rules. The specific disciplinary action depends upon the nature of the violation, the impact of the violation on Telkomsigma's informational assets and related facilities.

Depending on the violation, a Security Incident Report may be required to responsible entities and access privileges for user accounts involved in a compromise may be revoked during the time when a suspected violation is under investigation. Automated violation reports generated by the various security systems must be forwarded to the appropriate management for resolution.

B.3. Structure of This Document

The following chapters relate to logical groupings. Within each chapter there are appropriate sub-chapters which again, group related items. Following these are the individual Information Security Policies, which have been developed keeping in mind industry best practices.

B.4. Implementation and Compliance with the Policies

Implementation, compliance and follow up are now required. The Information Security Policies have established the ground rules across a wide range of Information Security areas. But translating these into a meaningful and practical response to the various day-to-day situations by user personnel can be a challenge. The most important aspect of Information Security Policy compliance is: knowing what actions are required to constitute 'compliance'. User organization must either develop its own range of procedures or consider using a tool specially crafted for the job.

In addition, the requirements of the policies must result in the need to initiate one or more Information Security Projects to identify and implement a range of appropriate technical safeguards such as firewalls, antivirus software, intrusion detection systems, etc.

C. Information Security Policies

C.1. Management direction for information security

1. All Telkomsigma information, in any form or format, must be used for appropriate business, and must be protected since its creation, through its useful life, until the authorized disposal. It also must be regularly maintained and be readily available anytime for authorized use.
2. Each authorized user of Telkomsigma information has an obligation to preserve and protect Telkomsigma's assets in a consistent and reliable manner. Security controls provide the necessary physical and procedural safeguards to accomplish those goals.
3. Telkomsigma top management is responsible for ensuring appropriate controls are in place to preserve the security objectives of confidentiality, integrity, and availability for Telkomsigma information assets.
4. Top management must approve, publish, and communicate this policy to all Telkomsigma employees, contractors and third party users.

C.2. Review of the policies for information security

1. The owner of Telkomsigma information security policy is responsible for development, review, and evaluation of the information security policy.
2. The review must include assessing opportunities for improvement of the policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.
3. Management approval must be obtained whenever there is policy revision.

D. Organization of Information Security

D.1. Internal Organization

D.1.1. Information security roles and responsibilities

1. Security roles and responsibilities of Telkomsigma employees, contractors and third party users must be defined during pre-employment process, and must consider the following requirements:
   a. Align with Telkomsigma information security policies
   b. Protect assets from threat of confidentiality, integrity, and availability
   c. Execute particular security processes or activities
   d. Report any security events or risk to Telkomsigma
2. Job descriptions must define security roles and responsibilities. Security responsibilities must be included in third-party contracts, and monitored during the engagement.

D.1.2. Segregation of duties

1. Segregation of duties must be implemented to prevent unauthorized or unnecessary disclosure in accordance with confidentiality and privacy requirements.
2. No single person can access, modify or use assets without detection and authorization.

D.1.3. Contact with authorities

1. Telkomsigma must have in place, contact with relevant authorities, such as fire department, law enforcement, supervisory authorities, internet service provider, or telecommunication operator when there is requires their action.
2. The process must include when to contact the authorities, whom to contact, and how to report the incident.

D.1.4. Contact with special interest groups

1. Contact or membership in special interest groups or forums must be seen as a mean to improve knowledge and staying up to date, also to improve cooperation and coordination of security issues.
2. Information sharing agreements must establish to protect sensitive information.

D.1.5. Information Security in Project Management

1. Information security is one of the aspects that is must be considered, identified and addressed in project management.
2. Project management must be integrated in Telkomsigma project management methodology. Implications of information security must be addressed and reviewed regularly.

D.2. Mobile Devices and Teleworking

D.2.1. Mobile Devices

1. When using mobile devices, e.g.~~, ~~notebooks, ~~palmtops, ~~laptops, special care must be taken to ensure that business information is not compromised. The mobile devices policy must take into account the risks of working with mobile devices equipment in unprotected environments
2. The mobile devices that owned by Telkomsigma's employees or NOP Telkomsigma mobile devices must be scanned by appointed Information Security officer when use in restricted area
3. Care must be taken when using mobile devices facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. The Protection must be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.
4. Users of mobile devices facilities in public places must take care to avoid the risk of overlooking by unauthorized persons.
5. Back-ups of critical business information must be taken regularly. Equipment must be available to enable the quick and easy back-up of information. These back-ups must be given adequate protection against, e.g., theft or loss of information.
6. Suitable protection must be given to the use of mobile facilities connected to networks.
7. Remote access to business information across public network using mobile devices facilities must take place after successful identification and authentication, and with suitable access control mechanisms in place.
8. Mobile devices facilities must be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres, and meeting places.
9. Equipment carrying important, sensitive, and/or critical business information must not be left unattended and, where possible, must be physically locked away, or special locks must be used to secure the equipment. The access control can be both physical and logical.
10. Training must be arranged for personnel using mobile devices to raise their awareness on the additional risks resulting from this way of working and the controls that must be implemented.

D.2.2. Teleworking

1. Organizations must authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy.
2. Suitable protection of the teleworking site must be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities.
3. Teleworking activities must both be authorized and controlled by management, and it must be ensured that suitable arrangements are in place for this way of working.

E. Human Resources Security

E.1. Prior to Employment

E.1.1. Screening

1. New employees, including external parties references must be carefully verified, and the employees must undertake to abide by Telkomsigma rules and regulations.
2. The past employment records of the new employee to be taken in the organization must be verified from the last organization.

E.1.2. Terms and Conditions of Employment

1. Each employee must sign a Non-Disclosure Agreement (NDA) on being recruited by the organization keeping in mind the employment terms (permanent, contractual, outsourced), position, and area of responsibility. Non-compliance with the NDA may lead to the severest action possible.
2. All employees must comply with the Information System Security Policies and procedures of Telkomsigma. Any information security incidents resulting from non-compliance must result in immediate disciplinary action.
3. All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with Telkomsigma.
4. Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Information Security Officer to prevent any damage to Telkomsigma.

E.2. During Employment

E.2.1. Management Responsibilities

1. Telkomsigma management is responsible to ensure all Telkomsigma employees, contractors and third party users are properly briefed on their information security roles and responsibilities before being granted access to sensitive information and information system.
2. The management must ensure that everyone is motivated to fulfill Telkomsigma security policies and therefore reduce the likelihood of policy violation and information security breach.

E.2.2. Information Security Awareness, Education and Training

1. All employees are to be provided with Information Security awareness training to enhance awareness and to leverage their consciousness regarding the range of security threats and the appropriate safeguards.
2. A document describing the information security responsibilities must be followed by all employees, contractors and third parties.
3. Proper mentoring must be provided to all employees to make them aware of their incompliance with the information security policies and procedures and to ensure that they are aware of the corrective measures.
4. Information security training must be provided to all employees to maintain their awareness of information security risks during new employee induction session and when their job responsibilities are changed.

5. Regular training must be provided to all employees to update them with the changes in the information security policies.
6. Periodic training for the appointed Information Security Officer must be prioritized to update his/her knowledge in the latest security threats and techniques. MS and/ or Telkomsigma management must evaluate the effectiveness of training provided internally and externally to ensure that the right person is given the right training and at the right time.
7. Information Security awareness training must be provided at least once in a year to employees in IT Operation services unit.

E.2.3. Disciplinary Process

1. The formal disciplinary process must ensure correct and fair treatment for employees who are suspected of committing breaches of security.
2. For serious cases, the disciplinary process must range from removal of access rights to termination of employment. Additionally, disciplinary process can also be used to prevent employees, contractors, and third party users from violating Telkomsigma information security policies and procedures.

E.3. Termination and Change of Employment

1. Upon notification of employee promotion, demotion, mutation, termination or resignation, Human Resources management must coordinate with the appointed Information Security Officer to detail the employee’s access rights and subsequently revoke the rights.
2. Checks must be done that no logical and physical access rights, and assets are still in the employee’s custody. The employee must be released from his job only after he has submitted all Telkomsigma’s assets and/ or properties provided during employment.
3. System and information access rights of employees who are transferring to competitors or leaving the office for a certain period must be terminated immediately.

F. Asset Management

F.1. Responsibility for Asset

F.1.1. Inventory of Asset

1. Telkomsigma must identify all assets and document the importance of these assets. The inventory must include all information necessary to recover from disaster, including type of asset, format, location, backup information, license information, and a business value.
2. An adequate level of asset protection must be identified based on the importance of the asset.

F.1.2. Ownership of Asset

1. Creator of information assets is the default assets owners and must be responsible for the determination of its classification.
2. Information owners must designate custodian to be responsible for safeguarding the information's CIA (confidentiality, integrity, and availability).
3. Custodian must not grant any access to the information to anyone without written permission from the owner.
4. An owner must notify his/ her custodian if the information assets are no longer required or valid.

F.1.3. Acceptable Use of Asset

All employees, contractors, and third party users are required to follow the rules for the acceptable use of information and assets associated with information processing facilities, including rules for email and internet usage, and guidelines for the use of mobile devices, especially the use of mobile devices outside Telkomsigma premises.

F.1.4. Return of Asset

The company assets that must be returned upon employment termination include all previously issued software, corporate document, equipment, and any other company asset such as mobile devices (laptop, mobile phone devices, etc), credit cards, access cards, keys, manuals, information stored on electronic media, etc.

F.2. Information Classification

F.2.1. Classification of Information

1. All information assets must be identified, recorded, and maintained in an information assets database by the respective owners.
2. All information must be classified according to their level of sensitivity, value, and criticality by the respective owners.
3. Telkomsigma must protect and ensure that the client confidentiality information must not be revealed to a third party without the consent of the client or a clear legal reason.
4. Any information asset must be classified into one of the classes below:

	Public	Internal use	Restricted	Confidential
Risk level	None	Routine (some impact/acceptable risk but do not any damage impact)	Moderate (damge / be prejudicial)	Grave damage
Sensitivity level	Open or unclassified	Low – Medium	Moderate – High	High
Definition	Public information is information that can be disclosed to anyone without violating an individual's right to privacy. Knowledge of this information does not expose Telkomsigma to financial loss, embarrassment, or jeopardize the security of asset.	Internal use information is information that, due to technical or business sensitivity, is limited to employees of Telkomsigma. Unauthorized disclosure, compromise, or destruction would not have a significant impact on Telkomsigma or its employee. Customer or vendor/related third party is allowed on-site view the information with the authorized permittion / document owner.	Restricted information is information that Telkomsigma and its employees have legal,regulatory, or social obligation to protect. The information is accessible to certain employees of Telkomsigma.	Confidential information, the highest level of classification, is information whose unauthorized disclosure, compromise, or destruction result grave damage to Telkomsigma, its customers, share holders, such as provide significant advantage to a competitor or loss financial impact or company image to Telkomsigma.
Accessible	• Public	• Employees of Telkomsigma	• Certain employees (as organization structure design)	• Management level or management representative
e.g.	• Press release • Marketing brochures • Interviews with news media	• Policies and standards • Organization charts • Employee handbook • Daily operation checklist	• Customer records • Employee records • Quatation precalc • Service catalog • Encryption keys • Access Password/PIN • Specific Policies and standards	• Strategy Plan • Business Plan • Business Continuity Plan • Product roadmap • Partnership scheme • AKI

F.2.2. Labeling of Information

1. Information assets must be clearly labeled so that users are aware of the ownership and classification of the information.
2. Information assets must be labeled according to the information classes.

F.2.3. Handling of Assets

1. Information assets must be processed, transmitted, and stored strictly in accordance with the classification levels assigned to the information.

F.3. Media Handling

F.3.1. Management of Removable Media

All Telkomsigma's stakeholder must protect Telkomsigma's information regardless of the media upon which it is maintained. Removable media includes tapes, disks, CDs, DVDs, Flash disks, removable hard drives, and printed media.

F.3.2. Disposal of Media

1. Media containing sensitive information must be stored and disposed securely and safely, e.g. by incineration or shredding, or erased of data using technical method.
2. The use of third party to handle secure media disposal must be selected carefully.
3. Disposal of sensitive items must be logged where possible in order to maintain an audit trail.

F.3.3. Physical Media Transfer

1. Media being transported must be protected from unauthorised access, misuse or corruption.
2. Authorized and reliable transport or courier must be used and control must be adopted to protect the information from unauthorized disclosure or modification.
3. The list of authorized couriers must be agreed with management, and procedures for couriers identification check must be developed.
4. The packaging of information media must be sufficient to protect the contents from any physical damage and in accordance with manufacturer's specification.
5. The Information that's classified as Confidential or higher classified, must be passworded or encrpyted to external parties.

G. Access Control

G.1. Business Requirement Access Control

G.1.1. Access Control Policy

1. Access control standards for information systems must be established by Management and the Information Security Officer and must incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.
2. Access control standards are set out by addressing the followings:
   a. The sensitivity level of the data being processed by all business systems and their appropriate level of access control.
   b. The dissemination/ circulation of information stored by specific systems.
   c. The consistency of user profiles across applications and their underlying operating systems.
   d. The requirements for compliance with legal and regulatory controls.
3. User access rights for all IT Operation service systems must be reviewed on a periodic basis. The appointed Information Security Officer is responsible for coordinating the activity.
4. The appointed Information Security Officer must established formal user registration and de-registration procedures in place
5. Access to all systems and premises must be authorized by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in access control matrix. Such records are to be regarded as restricted documents and safeguarded accordingly by the appointed Information Security Officer.
6. Equipment must always be safeguarded appropriately – especially when left unattended.
7. Administrator password in all IT components must be set by the appointed Information Security officer and kept in a dedicated storage.
8. Administrator account must be limited in number.
9. No external party is allowed to connect to internal Telkomsigma's IT resources without written consent from the appointed Information Security officer.

G.1.2. Access to Network and Network Services

1. Telkomsigma must establish a standards or procedures on the use of network services that defines which network and network services are allowed for each user group.
2. Authorization of access to Telkomsigma network and network services must be determined.

G.2. User Access Management

G.2.1. User Registration and De-Registration

1. A formal user registration and de-registration process must be implemented to enable assignment of access rights. The criteria of user access management must include :
   a. Using unique user IDs to enable users to be linked to and held responsible for their actions.
   b. Checking that the user has authorization from the system owner for the use of the information system or service.
   c. Checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy, e.g. it does not compromise segregation of duties.
   d. Immediately removing or blocking access rights of users who have changed roles or jobs or left the organization.

G.2.2. User Access Provisioning

A formal user access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services. The process user access provisioning must include :

a. Authorizarion process from information system or service owner for the use of the information system or service.
b. Verification on the level of access granted that is aligned with the user access matrix.
c. Process of adapting access rights for users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organization.
d. Periodically reviewing access rights with owners of the information systems or services

G.2.3. Management of Privileged Access Rights

1. Allocation of privilege must be established on a need-to-use basis, and provided only to meet the minimum requirement for the functional role needed.
2. The authorization process and record of all privilege allocated to user must be maintained and retained.
3. The need to use privilege must be minimized when possible, by developing and using system routines and programs.

G.2.4. Management of Secret Authentication Information of Users

1. Users are required to sign a statement to keep personal password confidential, and group password must only be kept within the members of the group.
2. Prior to providing a new, replacement or temporary password, the identity of a user must be verified.

3. Initial or temporary password for user must be provided in a secure manner and user must change the password immediately. The temporary password must be unique to an individual and not guessable.
4. When installing new system and software, default vendor password must be changed

G.2.5. Review of User Access Rights

1. User access right must be reviewed at regular intervals and after any employment changes, such as promotion, demotion, mutation, or termination.
2. Review for special privileged access rights must be done at more frequent interval.
3. Changes for privileged accounts must be logged for periodic review.

G.2.6. Removal or Adjustment of Access Rights

1. The access rights include physical and logical access, such as keys, identification cards, information processing facilities subscriptions, and system logins. Any documentation that identifies the employee as current member of company or department must be updated.
2. If the leaving employee has known passwords for accounts that remain active, the passwords must be changed upon termination of employment.
3. Upon employment change or employee mutation to another department or change responsibility, only relevant access right may be retained, any other access right that is not relevant with the new responsibility must be removed.

G.3. User Responsibilities

G.3.1. Use of Secret Authentication Information

1. All of Telkomsigma users must be advised to:
   a. Keep their password confidential.
   b. Select password with sufficient length that is easy to remember but hard to guess.
   c. Change temporary password at first log on.
   d. Change password regularly or whenever there is any indication of possible password compromise.
   e. Avoid writing down password (on paper or files) unless it can be stored securely.
   f. Not include password in any automated log-on process, e.g, stored in a macro or function key.

G.4. System and Application Access Control

G.4.1. Information Access Restriction

1. The Superuser account's password on all of IT Operation service systems must be maintained under dual custodian and kept in the vault.

2. Telkomsigma must not be responsible for maintaining superuser account's password that belong to customer.
3. Data directories and structures must be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories must be applied as necessary to restrict unauthorized access.

G.4.2. Secure Log-on Procedures

1. The process for logging into an operating system must be designed to minimize the opportunity for unauthorized access.
2. The log-on process must, therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

G.4.3. Password Management System

A password management system must :

1. Enforce the use of individual user IDs and passwords to maintain accountability
2. Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors
3. Enforce a choice of quality passwords, which can be done by enforcing password criteria
4. Enforce password changes periodically
5. Force users to change temporary passwords at the first log-on
6. Maintain a record of previous user passwords and prevent re-use for
7. Not display passwords on the screen when being entered
8. Store password files separately from application system data
9. Store and transmit passwords in protected form, e.g encrypted or hashed

G.4.4. Access Control to Program Source Code

1. Where possible, program source libraries must not be held in operational systems
2. The program source code and the program source libraries must be managed.
3. Support personnel must not have unrestricted access to program source libraries.
4. The updating of program source libraries and associated items, and the issuing of program sources to programmers must only be performed after appropriate authorization has been received
5. Program listings must be held in a secure environment
6. An audit log must be maintained of all accesses to program source libraries
7. Maintenance and copying of program source libraries must be subject to strict change control procedures

H. Physical and Environment Security

H.1. Secure Areas

H.1.1. Physical security Perimeter

Telkomsigma must ensure that IT and Network facilities supporting critical or sensitive business activities are housed in secure areas to prevent unauthorized access, damage and interference to IT and Network services. Physical security protection must be based on defined physical security perimeters.

1. Physical protection must be achieved by creating one or more physical barriers around Telkomsigma premises and information processing facilities.
2. Additional barriers and perimeter to control physical access must be needed between areas with different security requirements inside the security perimeter.
3. For buildings that are shared with other company or organization, there must be special consideration towards physical access security.

H.1.2. Physical Entry Control

1. Access control system must be available 24 hours a day and 7 days a week.
2. Doors must always be properly closed.
3. Users must be provided with access to the working area that they have been specially authorized to enter.
4. Access control system must be centralized.

H.1.3. Securing offices, room and facilities

Securing offices, rooms, and facilities must take into account health and safety regulations and standards.

1. Key facilities must be sited to avoid access by public.
2. Where applicable, buildings must be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying information processing activities.
3. Directories or internal telephone books identifying location or sensitive information processing facilities must not be readily accessible by public.

H.1.4. Protecting against external and environment threats

Hazardous or combustible materials must be stored at a safe distance from a secure area.

1. Bulk supplies such as stationery must not be stored within a secure area.
2. Fallback equipment and back-up media must be sited at a safe distance to avoid damage from a disaster affecting the main site.
3. Appropriate firefighting equipment must be provided and suitably placed.
4. To avoiding any security threats, consideration must also be given to neighboring premises, for example: fire in a neighboring building, water leaking from the roof or upper floors, or explosion in the street.

H.1.5. Working in secure areas

Personnel must be aware about the existence or activities within secure areas on a need to know basis.

1. Working without supervision in secure areas must be avoided both for safety reasons and to prevent opportunities for malicious activities. This applies to contractors, and third party users.
2. Vacant secure areas must be physically locked and periodically checked.
3. Photographic, video, audio or other recording equipment, such as cameras in mobile devices, must not be allowed, unless authorized.

H.1.6. Delivery and loading area

1. An intermediate ~~holding~~ loading area must be considered for deliveries to information processing facilities.
2. Access to a delivery and loading area from outside of the building must be restricted to identified and authorized personnel.
3. The delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building.
4. The external doors of a delivery and loading area must be secured when the internal doors are opened.
5. Incoming material must be inspected for potential threats before this material is moved from the delivery and loading area to the point of use.
6. Incoming material must be registered in accordance with asset management procedures on entry to the site.
7. Incoming and outgoing shipments must be physically segregated, where possible.

H.2. Equipment

H.2.1. Equipment sitting and protection

1. Equipment must be sited to minimize unnecessary access into work areas
2. Information processing facilities handling sensitive data must be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access
3. Items requiring special protection must be isolated to reduce the general level of protection required
4. Controls must be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.
5. Environmental conditions, such as temperature and humidity, must be monitored for conditions, which adversely affect the operation of information processing facilities
6. Lightning protection must be applied to all buildings and lightning protection filters must be fitted to all incoming power and communications lines
7. Equipment processing sensitive information must be protected to minimize the risk of information leakage due to emanation

H.2.2. Supporting Utilities

1. Fire detection and suppression system must be available in machine rooms and information processing premises.
2. Fire detection and suppression system must be maintained periodically.
3. The electric power supply must be backed-up by uninterruptible power supply and Genset.
4. UPS/ backup battery must be installed to ensure the continuity of services during power outages.
5. The UPS, Genset, backup battery, and system health must be maintained and checked regularly.
6. All electric power supply equipment must be placed in secure area.

H.2.3. Cabling Security

1. Cabling must be installed properly and maintained to ensure the integrity of both the cabling and the wall-mounted sockets.
2. Cables must be labelled and placed in tray.
3. Unused cable must be unplugged.

H.2.4. Equipment Maintenance

1. Equipment must be appropriately maintained in accordance with supplier's recommendation on service intervals and specifications.
2. To carry out repairs and service equipment, only authorized maintenance personnel are allowed.
3. Records must be kept for all faults (suspected or actual) and maintenance (preventive and corrective).
4. Appropriate controls must be implemented when equipment is scheduled for maintenance.
5. Whenever necessary, sensitive information must be cleared from the equipment, and the maintenance personnel must be sufficiently cleared.

H.2.5. Removal of Assets

1. Equipment, information or software must not be taken off-site without prior authorization.

2. Employees, contractors and third party users who have authority to permit off-site removal of assets must be clearly identified.

3. Time limits for equipment removal must be set and returns checked for compliance.

4. Where necessary and appropriate, equipment must be recorded when being removed off-site and recorded when returned.

H.2.6. Security of equipments off-premises

1. Security risks of working outside premises, such as theft, damage, or eaves-dropping, may vary considerably between locations.
2. Adequate insurance coverage must be in place to protect equipment off-site.
3. Equipment and media taken off premises must not be left unattended in public places.
4. Portable computers must be carried as hand luggage and disguise if possible when traveling.

H.2.7. Secure disposal or reuse of equipment

1. Because information can be compromised through careless disposal or re-use of equipment, sensitive information must not be deleted using only standard delete or format function.
2. Devices containing sensitive information must be physically destroyed, or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable.

H.2.8. Unattended user equipment

All Telkomsigma users must -:

1. Terminate active sessions when finished.
2. Log off computers when the session is finished.
3. Secure PCs or terminals from unauthorized access by a key lock or password.

H.2.9. Clear desk and clear screen policy

All Telkomsigma Users must be advised to :

1. Store papers and other storage media (–USB Drive, Portable Hard disk, DVD, etc) in cabinets when not in use.
2. Lock away sensitive program information when not in use, particularly when an office is vacated.
3. Workstations must be protected from unauthorized physical access.
4. When printing or scanning documents containing sensitive information, the print out must be removed from printers or scanners immediately.
5. Incoming and outgoing mail points and facsimile machines must be protected.

I. Cryptography

I.1. Cryptographic Controls

I.1.1.Policy on The Use of Cryptographic Controls

When using cryptographic controls the following must be considered:

1. The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information must be protected.
2. Based on a risk assessment, the required level of protection must be identified taking into account the type, strength, and quality of the encryption algorithm required
3. The use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines
4. The approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys
5. Roles and responsibilities for the implementation of the cryptographic control and key management
6. The standards to be adopted for the effective implementation (which solution is used for which business processes)
7. The impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

J. Operations Security

J.1. Operational procedures and responsibility

J.1.1. Documented operating procedures

1. Documented procedures must be prepared for system activities associated with information processing and communication facilities, such as system start-up and close-down procedure, backup, background job monitoring, equipment maintenance, problem handling, computer room security, media handling management, and safety.
2. These documents must be maintained and kept up to date for any changes. Documents accessibility and availability must be based on need-to-know principle.

J.1.2. Change management

1. All changes to production environment include end point devices (e.g., workstation, wireless connections etc) must be properly assessed, authorized, tested and implemented, and documented to provide audit trail.

J.1.3. Capacity Management

1. Capacity requirements must be identified for each new and ongoing activity.
2. Capacity requirements must be monitored to avoid failures due to inadequate capacity.
3. System tuning and monitoring must be applied to ensure and, where necessary, improve the availability and efficiency of systems.
4. Detective controls must be put in place to indicate problems in due time.
5. Advance planning and preparation are required to ensure the availability of adequate capacity and resources to minimize the risk of systems failure.
6. Projections of future capacity requirements must take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.
7. Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers must monitor the utilization of key system resources.
8. They must identify trends in usage, particularly in relation to business applications or management information system tools.
9. Managers must use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

J.2. Protection from malware

J.2.1. Controls against malware

1. Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across servers, PCs, and laptop computers.
2. Machine containing virus must be qua~~r~~rantined immediately from the network followed by virus removal.
3. Only authorized personnel are allowed to execute virus scanning and removal.

J.3. Backup

J.3.1. Information backup

1. Information system owners must ensure that adequate back up and system recovery procedures are in place.
2. Full system backup must be stored to backup media regularly.
3. Information and data stored on servers, computers, and laptops must be backed up regularly to prevent corruption or loss through system or power malfunction.
4. Backup of the organization's data files and the ability to recover such data is important. The appointed Information Security Officer is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.
5. Tape backup must be deposited by the Librarian Team.

J.4. Logging and monitoring

J.4.1. Event logging

1. Log record in all systems must be enabled including error logs and audit logs to provide evidence of security events and negligence.
2. All logs including error logs and operational audit logs must be properly reviewed with evidence of such review documented.
3. Retention of logs must be based on contractual business requirements.

J.4.2. Protection of log information

1. Controls must be established to protect against unauthorized changes and operational problems with the logging facility.
2. Some audit logs may be required to be archived as part of contractual business requirements because of requirements to collect and retain evidence.

J.4.3. Administrator and operator log

Log of system administrator and system operator activities must be activated and reviewed regularly.

J.4.4. Clock synchronization

1. System clocks must be synchronized regularly especially between the organization's various processing platforms.
2. The appointed Information Security Officer must check and correct any significant variation.
3. Unless formally requested and agreed by both parties (Telkomsigma and external customer), the time system that is applied at Telkomsigma is based on Telkomsigma's main NTP server located.

J.5. Control of operational software

J.5.1. Installation of software on operational systems

To minimize the risk of corruption to operational systems, the following guidelines must be considered to control changes:

1. The updating of the operational software, applications, and program libraries must be performed by trained administrators upon appropriate management authorization.
2. Operational systems must hold approved executable code, and not development code or compilers.
3. Applications and operating system software must be implemented after extensive and successful testing. The tests must include tests on usability, security, effects on other systems and user-friendliness, and must be carried out on separate systems. It must be ensured that all corresponding program source libraries have been updated.
4. A configuration control system must be used to keep control of all implemented software as well as the system documentation.
5. A rollback strategy must be in place before changes are implemented.
6. An audit log must be maintained of all updates to operational program libraries.
7. Previous versions of application software must be retained as a contingency measure.
8. Old versions of software must be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive

J.6. Technical vulnerability management

J.6.1. Management of technical vulnerabilities

1. A current and complete inventory of assets is a prerequisite for effective technical vulnerability management.
2. Information resources that must be used to identify relevant technical vulnerabilities and to maintain awareness about them must be identified for software and other technology (based on the asset inventory list).
3. Appropriate and timely action must be taken in response to the identification of potential technical vulnerabilities.

J.6.2. Restriction on software installation

1. The organization must define and enforce strict policy on which types of software users may install.
2. The principle of least privilege must be applied.

J.7. Information system audit considerations

J.7.1. Information system audit control

1. Audit requirements must be agreed with appropriate management.

2. The scope of the checks must be agreed and controlled.

3. The checks must be limited to read-only access to software and data.

4. Access other than read-only must only be allowed for isolated copies of system files, which must be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.

5. Resources for performing the checks must be explicitly identified and made available.

6. Requirements for special or additional processing must be identified and agreed.

7. All access must be monitored and logged to produce a reference trail; the use of time-stamped reference trails must be considered for critical data or systems.

8. All procedures, requirements, and responsibilities must be documented.

9. The person(s) carrying out the audit must be independent of the activities audited

K. Communication Security

K.1. Network security management

K.1.1. Network control

1. The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.
2. Hardware and operating system, networks, and communication systems must be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.
3. Wireless connection must be strictly controlled in Data Center premises.
4. Wireless network scan must be performed using on a quarterly basis.
5. Network configuration must be tested and reported regularly (e.g. penetration test reports, vulnerability scanning reports). Tools to conduct the test must be limited and kept in secure location.
6. Any configuration change must be properly documented, including its impact analysis.
7. Network diagrams with complete information be maintained by the Network Operation team.

K.1.2. Security of network services

1. Security features, service levels, and management requirements of all network services must be identified and implemented.
2. The ability of the network service provider to manage agreed services in a secure way must be determined and regularly monitored, and the right to audit must be agreed.

K.1.3. Segregation in network

1. Networks must be divided into separate logical network domains, each protected by a defined security perimeter.
2. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the organization.
3. Networks must be segregated using the network device functionality.

K.2. Information transfer

K.2.1. Information transfer policies and procedures

1. Procedures and protocols must be in place to protect the exchange of information through any format e.g. email, video, fax, or direct. communication.
2. The procedures must be designed to protect exchanged information from: interception, copying, modification, mis-routing, destruction.
3. Information must be protected with appropriate controls based on the information's classification.

K.2.2. Agreements on information transfer

1. Formal agreements for the exchange of information must refer to company policies, procedures, and standards to protect information and physical media in transit.
2. Agreements may be electronic or manual, and may take the form of formal contracts or conditions of employment.
3. For sensitive information, the specific mechanisms used for the exchange of such information must be consistent for all organizations and types of agreements.

K.2.3. Electronic messaging

Electronic messaging such as email, play an increasingly important role in business communications. Electronic messaging has different risk than paper based communication, thus requires different security consideration. The security consideration for electronic messaging must include:

1. Protecting messages from unauthorized access, modification or denial of service.
2. Ensuring correct addressing and transportation of the message.
3. General reliability and availability of the service.
4. Regulatory and contractrual business requirement.
5. Obtaining approval prior to using external public services such as instant messaging or file sharing.
6. Stronger levels of authentication controlling access from publicly accessible networks.
7. Ensure is only used for the company's business activities or purpose.

K.2.4. Confidentiality or non-disclosure agreement

1. Users of Telkomsigma information processing facilities must sign a confidentiality agreement.
2. Confidentiality or non-disclosure agreements protect organizational information and inform the signatories of their responsibility to protect, use, and disclose information in a responsible and authorized manner.

L. System acquisition, development and maintenance

L.1. Security requirement of information systems

L.1.1. Information security requirement analysis and specification

1. Specifications for the requirements for controls must consider the automated controls to be incorporated in the information system, and the need for supporting manual controls. Similar considerations must be applied when evaluating software packages, developed or purchased, for business applications.
2. Security requirements and controls must reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security.
3. System requirements for information security and processes for implementing security must be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.
4. If products are purchased, a formal testing and acquisition process must be followed.
5. Contracts with the supplier must address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls must be reconsidered prior to purchasing the product.
6. Where additional functionality is supplied and causes a security risk, this must be disabled or the proposed control structure must be reviewed to determine if advantage can be taken of the enhanced functionality available.

L.1.2. Securing application services on public network

1. Telkomsigma must establish control to protect the integrity of the information being made available on a publicly available system.
2. Formal approval is required before the information is made available.
3. Test against weakness and failures must be conducted prior to deploying publicly available system and all input from outside to the system must be verified.

L.1.3. Protecting application services transactions

1. Security control must be applied to protect information involved in on-line transaction from incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
2. Protocol used to communicate between all involved parties must be secured, and the communication path must be encrypted. The storage of the transaction details must be located outside of any public accessible environment.

L.2. Security in development and support processes

L.2.1. Secure development policy

1. Secure programming techniques must be used both for new developments and in code re-use scenarios.
2. If development is outsourced, the organization must obtain assurance that the external party complies with these rules for secure

L.2.2. System change control procedures

1. Formal change control procedures must be documented and enforced in order to minimize the corruption of information systems.
2. Introduction of new systems and major changes to existing systems must follow a formal process of documentation, specification, testing, quality control, and managed implementation.
3. This process must include a risk assessment, analysis of the impacts of changes, and specification of security controls needed.
4. This process must also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

L.2.3. Technical review of application after operating system changes

This process for operating system changes must cover:

1. Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes
2. Ensuring that the annual support plan and budget must cover reviews and system testing resulting from operating system changes.
3. Ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation.
4. Ensuring that appropriate changes are made to the business continuity plans.
5. A specific group or individual must be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

L.2.4. Restriction on changes to software packages

1. As far as possible, and practicable, vendor-supplied software packages must be used without modification.
2. If changes are necessary the original software must be retained and the changes applied to a clearly identified copy.
3. A software update management process must be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software.
4. All changes must be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

L.2.5. Secure system engineering principles

1. Secure information system engineering procedures based on security engineering principles must be established, documented and applied to in-house information system engineering activities.
2. If changes are necessary the original software must be retained and the changes applied to a clearly identified copy.

L.2.6. Secure development environment

Telkomsigma must document corresponding processes in secure development procedures and provide these to all secure information system engineering procedures based on security engineering principles must be established, documented and applied to in-house information system engineering activities.

L.2.7. Outsourced development

The followings must be considered in outsourced software development:

1. Licensing arrangements, code ownership, and intellectual property rights
2. Certification of the quality and accuracy of the work carried out.
3. Escrow arrangements in the event of failure of the third party
4. Rights of access for audit of the quality and accuracy of work done.
5. Contractual requirements for quality and security functionality of code.
6. Testing before installation to detect malicious and Trojan code

L.2.8. System security testing

1. New and updated systems require thorough testing and verification during the development processes.
2. The extent of testing must be in proportion to the importance and nature of the system.

L.2.9. System acceptance testing

1. Requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested to confirm that all acceptance criteria have been fully satisfied.
2. New information systems, upgrades, and new versions must only be migrated into production after obtaining formal acceptance.
3. For major new developments, the operations function and users must be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design.

L.3. Test data

L.3.1. Protection of test data

The following guidelines must be applied to protect operational data, when used for testing purposes:

1. The access control procedures, which apply to operational application systems, must also apply to test application systems.
2. There must be separate authorization each time operational information is copied to a test application system.
3. Operational information must be erased from a test application system immediately after the testing is complete.
4. The copying and use of operational information must be logged to provide an audit trail.

M. Supplier relationships

M.1. Information security in supplier relationships

M.1.1. Information security policy for supplier relationships

Telkomsigma must identify and mandate information security controls to specifically address supplier access to the organization's information in a policy.

M.1.2. Addressing security within supplier agreements

1. The agreements must consider security requirements such as the information security policy, asset protection and control, responsibilities of each parties, access control policy, a clear process and reporting structure and format, target level of service and performance criteria, service continuity requirements, the rights to monitor and revoke any activity, etc.
2. The right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors.
3. The agreements must consider the conditions for renegotiation/termination of agreements.

M.1.3. Information and communication technology supply chain

1. Telkomsigma must work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided.
2. Telkomsigma have the authority to influence information and communication technology supply chain by making clear in agreements with suppliers the matters that must be addressed by other suppliers in the information and communication technology supply chain.

M.2. Supplier services delivery management

M.2.1. Monitoring and review of supplier services

1. The monitoring and review on third party services must ensure that information security terms and conditions of the agreements are being adhered to, and information security incidents are managed properly.
2. The management must appoint designated team to manage the relationship with third party.
3. Sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party must be maintained.

M.2.2. Managing changes to supplier services

The process of managing changes to third party services must take into account both the changes need to be made by Telkomsigma to implement, and changes in third party services to implement.

Changes made by the organization to implement could be:

1. Enhancements to the current services offered;
2. Development of any new applications and systems.
3. Modifications or updates of the organization's policies and procedures.
4. New controls to resolve information security incidents and to improve security.

Changes in third party services to implement:

1. Changes and enhancement to networks;
2. Use of new technologies;
3. Adoption of new products or newer versions/releases;
4. New development tools and environments;
5. Changes to physical location of service facilities;
6. Change of vendors.

N. Security Incident Management

N.1. Management of information security incident and improvement

Information security incident is the occurrence or development of an unwanted situation, which indicates either a possible breach of an information security framework policy or a failure of information security controls, which have significant probability of compromising business operations impact to internal and / or external.

N.1.1. Responsibilities and procedures

1. Incident that is categorized as information security incident must be identified, analyzed, corrected, communicated to functions affected, and reported to the appropriate authority.
2. Formal procedures must be established to handle different types of information security incident. Audit trails and similar evidence must be collected and secured, as appropriate, for internal problem analysis.
3. Action to recover from security breaches and correct system failures must be carefully and formally controlled.

N.1.2. Reporting information security events

1. A formal information security event reporting procedure must be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event.
2. A point of contact must be established for the reporting of information security events. It must be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.
3. All employees, contractors and third party users must be made aware of their responsibility to report any information security events as quickly as possible. They must also be aware of the procedure for reporting information security events and the point of contact.

N.1.3. Reporting information security weaknesses

1. All employees, contractors and third party users must report any observed or suspected security weaknesses to the appointed information security contact as quickly as possible in order to prevent information security incidents from happening.
2. The reporting mechanism must be as easy, accessible, and available as possible.
3. They must be informed that they must not, in any circumstances, attempt to prove a suspected weakness.

N.1.4. Assessment of and decision on Information Security Events

1. All Operation Monitoring team must respond rapidly but calmly to all reported information security events.
2. Any information security events must be investigated and reported on a timely basis.
3. Evidence relating to a suspected information security breach must be formally recorded and processed.
4. Information security events logs must be maintained and continually updated.

N.1.5. Response to Information Security Incident

1. Any information security incidents must be handled with corrective action.
2. Preventive action must be done in order to prevent security incident from re-occurring.

N.1.6. Learning from information security incidents

1. The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process.
2. The information gained from the evaluation of information security incidents must be used to identify recurring or high impact incidents.

N.1.7. Collection of evidence

1. Incident Response unit must collect and present evidence for the purposes of disciplinary action handled within an organization.
2. To achieve admissibility of the evidence, the information systems comply with any published standard or code of practice for the production of admissible evidence.
3. To achieve weight of evidence, the quality and completeness of the controls used must be considered to correctly and consistently protect the evidence.
4. The integrity of all evidence material must be protected.

O. Information security aspects of Business Continuity Management

O.1. Information security continuity

O.1.1. Planning information security continuity

1. Information security continuity is a part of Telkomsigma’s Business Continuity Plan.
2. Management must develop a business continuity plan, which covers all essential and critical business activities.
3. An up-to-date copy of the BCP must be stored in a secure location off-site.
4. During emergency conditions, only specially appointed spokesperson is permitted to speak to the media.
5. Emergency authorization processes must be established to enable recovery without unnecessary delay.
6. Event logs must be maintained.
7. BCP document must be treated as a restricted information.

O.1.2. Implementing information security continuity

1. Business continuity management process must address the information security requirement to counteract interruption to business activities and to protect critical business process for the effect of major failures of information system or disasters and to ensure their timely resumption.
2. Business continuity plan does not only address the organizational vulnerabilities but also the sensitive information that needs to be appropriately protected.
3. Each business continuity plan must describe the approach for continuity and also specify the escalation plan and levels include the conditions for its activation.
4. Each plan must have a specific owner, whom has the responsibility to manage appropriate business resources or processes involved.
5. Administration of business continuity plan adhere applicable Telkomsigma’s business continuity policy. When requirements are identified, they must be amended in appropriate procedure with the business owner.

O.1.3. Verify, review and evaluate information security continuity

1. The BCP is explained in more details and comprehensive on Telkomsigma BC policy and procedure documents.
2. The BCP must be tested in timely manner to ensure that the management and staff understand how it is to be executed.
3. The BCP must contain a description of the objectives and scope of the testing phase.
4. Review over the testing result must be performed to initiate improvement.

O.2. Redundancies

O.2.1. Availability of information processing facilities

Telkomsigma must identify business requirements for the availability of information systems and stated on BCP.

P. Compliance

P.1. Compliance with Legal and Contractual Requirements

P.1.1. Identification of applicable legislation and contractual requirement

1. Telkomsigma must fulfill security aspect stated in contract/ agreement with its customers.
2. Telkomsigma must follow laws, statutories, and regulatory obligations relevant to its customers as long as they are stated in contract/ agreement.
3. Management is responsible for ensuring that employees are aware of the key aspects of Copyright, Designs and Patents Act legislation (or its equivalent). All employees must aware of their legal obligations towards information security and the consequences of non-adherence.
4. The Legal Department must define employee legal obligations towards copyright.
5. All employees must fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the employee handbook.
6. Applicable legislation must be identified and ratified internally by process owner as adviced by Legal Deparment.
7. Data retention must be defined in accordance with statutory, regulatory, contractual and business requirements.

P.1.2. Intellectual Property Rights

Intellectual property rights including but not limited to software or document copyright, industrial design rights, trademarks, patents.

Proprietary software products are usually supplied under a license agreement that specifies license terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of back-up copies only. The IPR situation of software developed by Telkomsigma requires to be clarified with the staff.

Law and Regulation, and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by Telkomsigma, or that is licensed or provided by the developer to Telkomsigma, can be used. Copyright infringement can lead to legal action, which may involve criminal proceeding several guidelines to protect any material that may be considered intellectual property:

1. Publishing an intellectual property rights compliance policy, which defines the legal use of software and information products.
2. Acquiring software only through known and reputable sources, to ensure that copyright is not violated.
3. Maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them.
4. Maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights.
5. Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.

6. Implementing controls to ensure that any maximum number of users permitted is not exceeded.
7. Carrying out checks that only authorized software and licensed products are installed.
8. Providing a policy for maintaining appropriate license conditions.
9. Providing a policy for disposing or transferring software to others.
10. Using appropriate audit tools.
11. Complying with terms and conditions for software and information obtained from public networks.
12. Not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law.
13. Not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law

P.1.3. Privacy and protection of personally identifiable information

Telkomsigma systems may hold personally identifiable data, i.e., any data that is unique to any individual or company or data that is sensitive or proprietary to a Telkomsigma business partner. The protection of the privacy of this information is of utmost importance. Active steps must be taken by all Information Users to ensure privacy. All Telkomsigma personnel with access to personal information are required to respect the confidentiality of that private information. Telkomsigma's marketing and business processes must comply with the Law No. 11 Year 2008 concerning Information and Electronic Transaction, as well as other Law and Regulation requirements determined by the Telkomsigma Security Council to be necessary and prudent. Confidential or sensitive data, including information about Telkomsigma business, organizations and business partners, collected and maintained by Telkomsigma must:

1. Be used only for the stated purpose it was gathered.
2. Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose.
3. Not be disclosed without specific consent.
4. Be available for review by the individual or representative of the Telkomsigma information owner.
5. Be corrected if errors are known to exist or if the reviewer identifies errors.

P.1.4. Regulation of cryptographic controls

Legal advice must be sought to ensure compliance with national laws and regulations. Before encrypted information or cryptographic controls are moved to another country, legal advice must also be taken.

The following items must be considered for compliance with the relevant agreements, laws, and regulations:

1. Restrictions on import and/or export of computer hardware and software for performing cryptographic functions.
2. Restrictions on import and/or export of computer hardware and software, which is designed to have cryptographic functions added to it.
3. Restrictions on the usage of encryption.
4. Mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content

Q. Information security reviews

Q.1.1. Independent review of information security

1. The review must be carried out by independent individuals. These individuals can be internal audit function, an independent manager, or a third party organization specializing in such reviews.
2. The review result must be recorded and maintained. If the independent reviews identifies that Telkomsigma's approach is inadequate or not compliant with the direction as stated in the information security policy, then corrective action must be taken.

Q.1.2. Compliance with security policies and standards

1. Managers must regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.
2. If any non-compliance is found as a result of the review, managers must determine the causes of the non-compliance, determine and implement appropriate corrective action, and review the corrective action taken.
3. Managers must also evaluate the need for actions to ensure that non-compliance does not recur.
4. Results of reviews and corrective actions carried out by managers must be recorded and these records must be maintained.
5. Managers must report the results to the persons carrying out the independent reviews, when the independent review takes place in the area of their responsibility.

Q.1.3. Technical compliance review

1. Technical compliance checking must be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist.
2. If penetration tests or vulnerability assessments are used, caution must be exercised as such activities could lead to a compromise of the security of the system. Such tests must be planned, documented and repeatable.
3. Any technical compliance check must be carried out by competent, authorized persons, or under the supervision of such persons.

Definition	Description
Appointed Information Security Officer.	Assignee or an appointed officer in Information Security working unit that support operation and support
Evidence of Security Incidents.	the available body of facts or information indicating whether a belief or proposition is true or valid of a possible breach of information security or a security failure controls that can harm an organization's assets
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable latency data networks.
Information Security	The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
Information Security Events.	occurrence indicating a possible breach of information security or failure of controls
Information Security Incidents.	one or multiple related and identified *information security events* that can harm an organization's assets or compromise its operations
Incident Response unit.	The actions taken by the the appointed team whom has responsibility to mitigate or resolve an *information security incident*, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it
Operation Monitoring team.	a group of unit or department whom has responsibility to monitor the operation task (e.g. Network Operation, IT Security Operation, Facility Operation etc)
Network Operation team.	a group of network team which deliver daily task in operating network and network monitoring
Telkomsigma Security Council.	A group of management level whom have responsibility to review and to decide a security and risk issue in Telkomsigma