astragraphia
member of ASTRA

INFORMATION SECURITY POLICY

PT Astra Graphia Tbk

www.astragraphia.co.id

INFORMATION SECURITY POLICY

1. Purpose

1.1. Provide a framework related to the management of information security at Astragraphia.
1.2. Understand the responsibilities related to the protection of information assets at Astragraphia.
1.3. Protect Astragraphia employees in the event of misuse of information assets, loss or unauthorized disclosure of information.
1.4. Increase awareness of information security at Astragraphia.

2. Scope

2.1. This policy applies to all Astragraphia employees and everyone who has access to or manages information at Astragraphia.
2.2. Information security and Information Technology policies cover all systems, automatic and manual, for Astragraphia's administrative responsibilities. This includes all information, regardless of form and format, created or used to support Astragraphia's business processes.
2.3. Explain to Astragraphia employees the understanding and responsibilities regarding information security issues as an effort to protect Astragraphia's information assets.
2.4. Users/organizational structures who are given responsibility for managing this policy are Head of ITSS, Management (Board of Directors and Chiefs), Astragraphia Managers, Information Owners, Information Security Manager, Manage Services, Astragraphia Employees and external parties.
2.5. The policy must be communicated by the manager to all Astragraphia employees and all other people who have access to and manage Astragraphia information. This security policy is technology independent and does not include implementation standards, processes and procedures.

3. Definition

3.1. **ITSS** : Information Technology Shared Services
3.2. **Astragraphia** : PT Astra Graphia Tbk
3.3. **Information Security** : Efforts to protect asset security information.
3.4. **Incident Management** : Management of how to handle incidents that occurs.

4. Person in Charge

Dept. Head of ITSM is responsible for ensuring that the Information Security Policy is carried out correctly and appropriately in accordance with the applicable provisions and procedures.

5. Terms

5.1. Compliance Requirements

5.1.1. Compliance Requirements

Compliance to this policy is mandatory. Every employee must understand their roles and responsibilities regarding information security issues and protecting Astragraphia's information. Failure to comply with these or other security policies that result in compromise of Astragraphia's confidentiality, integrity, privacy and/or availability may result in disciplinary action or other actions in accordance with established procedures as set out in this policy, or other policies or policies and directives. Other relevant Astragraphia. Astragraphia will take every necessary step, including legal and administrative action, to protect its assets and has established the position of Information Security Manager to monitor compliance with policy matters.

5.1.1.1. **Exceptions to Policy**

The Head of Information Management must first approve any exceptions to this or other security policy or standard. The business case explaining the reasons for the exception must be documented in writing and submitted for approval by the Head of Information Management and must also be approved and kept by the person serving as the Information Security Manager. The person or organization that is excluded from the exception must also accept in writing all the risks associated with the exception.

5.1.1.2. **Enforcement Handling and Violation Handling**

Any compromise or suspected compromise to this policy must be reported to appropriate management and the Information Security Manager. All violations of security policies and/or standards are subject to disciplinary action or other appropriate actions in accordance with Astragraphia's policies.

Security incident reports indicating the level of risk of breach will be reported to the responsible entity. Access rights for user accounts involved in the compromise may be revoked while the alleged infringement is under investigation. Automatic breach reports generated by various security systems will be forwarded to appropriate management and Information Security Manager for timely resolution.

5.2. **Organizational and functional responsibilities**

The following is a brief description of the organizational structure responsible for managing this policy.

- **Head of Information Management:** Approve all changes to security policies and standards and resolve security issues when they conflict with business requirements.
- **Astragraphia Management (Board of Directors and Chief):** Will establish and support Astragraphia policies, including security policies and communicate these policies to Astragraphia employees.
- **Astragraphia managers:** will be responsible for the implementation of the policies and compliance of their staff under their supervision in its implementation, as stated in their mission statement. Managers should educate their staff regarding information security issues. The manager will explain the problem, why the policy has been established, and what role staff have in safeguarding information assets. The consequences of non-compliance should also be explained.
- **Information Owner:** The appointed manager will be the information owner for the data and tools they use. The owner of the information is responsible for determining who should have access to protected resources within his jurisdiction, and what access rights should be (read, update, etc.). These access rights must match the user's job responsibilities. The information owner also communicates with the Information Security Manager requirements to protect his data.
- **Information Security Manager:** The Information Security Manager is fully responsible for ensuring the implementation, improvement, monitoring and enforcement of the IT Information and Information Security Policy. The Information Security Manager is responsible for providing direction and leadership to Astragraphia through policy recommendations, standards and processes to ensure the proper level of security is implemented, and to ensure compliance with these policies, standards and processes. The Information Security Manager is responsible for investigating all suspected security breaches. The Information Security Manager will normally represent Astragraphia on all information security matters and will coordinate and oversee the security program activities and reporting processes to support this policy.

- **Service Manager** has a data processing infrastructure and a computing network that supports the owner of the information. It is the responsibility of these organizations to support the Information Security Policy and provide the resources needed to improve and maintain the level of information security controls that comply with the Information and IT Information Policy.
  The Service Manager has the following responsibilities with respect to information security:
  - ensure processes, policies and requirements are identified and implemented relative to the security requirements defined by the line of business;
  - ensure that appropriate information controls are implemented for business lines;
  - has assigned ownership responsibilities, based on the designation of the Astragraphia classification;
  - ensure the participation of the Information Security Manager and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and to protect information assets;
  - ensure that appropriate security requirements for user access to automated information;
  - define the files, databases and physical devices assigned to their area of responsibility;
  - ensure that critical data and recovery plans are backed up and stored in a safe place;
  - backup media storage, and recovery facilities will work as and when required;
  - ensure proper compliance with Astragraphia and other regulations and mission statements.
- **Astragraphia Employees:** It is the responsibility of all employees to protect Astragraphia's information and resources, including passwords, to record variances from established procedures, and to report variances or suspected security incidents to the appropriate manager and the Information Security Manager.
- **External Parties:** personnel of business partners, contractors, consultants, vendors and others, to the extent that their current or past access to AGIT's information assets is also covered by this policy.

5.3. Procedure References

The procedure refers to the provisions stipulated in Law Number 11 of 2008 concerning Information and Electronic Transactions and amendments thereto ("UU ITE"), Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data and Electronic Transactions (“Permen Perlindungan Data Pribadi”), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (“PP PSTE”).

5.4. Information Technology and Information Security Policy

All information regardless of the form or format created, obtained or used to support Astragraphia's business activities, may only be used for Astragraphia's business. Astragraphia information is an asset and must be protected from its creation, throughout its useful life. It must be kept safe, accurate, and reliable and available for lawful use.

5.4.1. Individual Accountability

Individual accountability is required when accessing all Astragraphia's electronic resources. Access to Astragraphia's computer systems and networks must be provided through the use of an individually assigned unique computer identifier, known as a user ID. Individuals, who use Astragraphia's computer resources can only access resources under their authority. Associated with each user-ID is an authentication token, such as a password, which must be used to authenticate the person accessing the data, system or network. Passwords should be treated as confidential information and should not be disclosed. All individuals are responsible for all activities performed with their user ID. For user protection, and to protect Astragraphia's resources, user IDs may not be shared.

5.4.2. Confidentiality/Integrity/Availability

- All Astragraphia information will be protected from unauthorized access to help ensure the confidentiality of information and maintain its integrity.
- Information will be made available for authorized use when required by the user in the normal course of his duties.
- A backup and restore schedule will be assigned to those systems and data to ensure timely recovery in the event of an extended outage.

5.4.3. Protection of Personal Data

Personal Data is certain personal data that is stored, maintained, and kept true and protected by confidentiality. Astragraphia respects the privacy of everyone including employees and customers and their Personal Data, including digital information about them that is stored by Astragraphia.

Astragraphia will collect and use Personal Data in accordance with Astragraphia's values, applicable laws and respect for privacy as a human right. This guiding policy sets out what steps should be taken to ensure Personal Data is handled appropriately. Socialization on the protection policy for Personal Data will be carried out periodically to all Astragraphia employees.

When collecting, using or storing Personal Data, employees must:

- Only collect sufficient and relevant data and use it solely for the purposes for which it was collected.
- Be transparent with individuals regarding how their Personal Data is used in accordance with applicable laws and regulations.
- Obtain permission from the individual in accordance with applicable law.
- Keep Personal Data up to date by correcting inaccurate information when requested.
- Maintain the confidentiality and security of Personal Data by limiting access to such Personal Data.
- Act responsibly and ethically, uphold Astragraphia's values, always consider the risks to individuals in using their Personal Data and take steps to reduce these risks.

When collecting, using or storing Personal Data, employees must not:

- Transferring Personal Data to anyone outside of the interested parties within Astragraphia.
- Collect and use Personal Data for purposes not expected by Astragraphia customers or employees.

5.5. Personnel Security Policy

The Personnel Security Policy is intended to reduce the risk of human error, theft or misuse of Astragraphia's information and facilities. Security responsibilities should be addressed at the employee recruitment stage and monitored during individual work. Potential individuals should have adequate background checks, especially if they are in a sensitive position. All employees and users of third-party information technology processing facilities must sign a nondisclosure agreement if they have access to sensitive information.

5.5.1. Personel Screening

Astragraphia follows the latest HR guidelines regarding pre-employment screening. Additional screening for position sensitive may be performed.

5.5.2. User Awareness

To ensure that all Astragraphia employees are aware of information security threats and issues, and are equipped to support Astragraphia's security policies, employees must be informed about security procedures and proper use of information processing facilities to minimize possible security risks.

All Astragraphia employees and where necessary third parties must receive regular updates in Astragraphia's security policies, standards and procedures. This includes security requirements, legal responsibilities and business controls, as well as the correct use of information facilities, such as login procedures and use of software packages, before access to information is granted.

An information security awareness program should be developed, implemented and maintained to meet the security education needs of all employees. Astragraphia's security awareness program will be strengthened at least annually.

5.5.3. Responding to Security Incidents and Malfunctions

Incidents affecting security must be reported to the Information Security Manager via the Help Desk (Customer Service Center/CSC) as soon as possible. All employees and contractors must be informed of the procedures for reporting various types of incidents (security breaches, threats, weaknesses or damages) that may impact the security of Astragraphia's assets.

5.5.4. Security Weakness Reports

Information technology users must be required to record and report any observed or suspected security weaknesses or threats such as intrusions from outside the Astragraphia area to the Information Security Manager. They should report this weakness as soon as possible. The user should not attempt under any circumstances to prove a suspected weakness. This is for their own protection because testing weaknesses can be considered a potential abuse of the system.

5.6. Physical and Environmental Safety Policy

Astragraphia's critical or critical business information processing facilities must be located in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls. They must be physically protected from unauthorized access, damage and interference.

5.6.1. Physical Security Perimeter

Physical security can be achieved by creating a physical barrier around the assets being protected. Each barrier forms a security perimeter that requires an access control method to enter. This perimeter can be an entrance with card key access, a reception area or other physical barrier. The risk assessment will determine the type and area of this perimeter.

5.6.2. Equipment Safety

Potential technical vulnerabilities must be identified and addressed by the IT team. Vulnerability management techniques should address vulnerability monitoring, vulnerability risk assessment, locating and tracking assets. A timeline should be defined in response to technical vulnerability notices. Procedures should be established to classify the level of action taken as technical vulnerabilities arise in relation to change handling procedures or incident handling procedures.

The risks associated with installing the Patch should be assessed. Patches must be tested before installing. If Patch is not available, then other controls should be considered:

a) Change the service associated with the vulnerability.
b) Adding access control.
c) Add monitoring to detect and prevent attacks.
d) Increase awareness of vulnerability.

Logs should be taken for all actions related to vulnerability fixing and/or patching and reviewed regularly. Appropriate technology should be used to assess technical vulnerabilities and should be audited annually.

5.6.3. Equipment Safety

Computer equipment must be physically protected from security threats and environmental hazards. Equipment protection is required to reduce the risk of unauthorized data access and to protect against loss or damage. Special controls may also be required to protect supporting facilities such as power supplies and wiring infrastructure.

5.6.4. Clean Desk and Clear Screen

Sensitive information as defined by the Astragraphia Data Classification standard must be removed from view and physically secured when not in use. Desktop and laptop computers should use screen savers to ensure sensitive information is not displayed after periods of user inactivity. Desktop computers connected to the network should log off automatically or lock screen after a certain period of inactivity.

5.7. Communication and Operations Management

5.7.1. Procedure and Operation

The operating procedures for all Astragraphia systems and applications must be documented and maintained. Operating procedures should be treated as formal documents and changes should be authorized by management. Documented procedures must also be prepared for household activities related to information and communication processing facilities such as computer startup and shutdown procedures, back-up, equipment maintenance, data center management and security.

5.7.2. Operation Change Control

Changes to Astragraphia's information processing facilities and systems must be authorized and controlled through a formal change management process. Formal management responsibilities and procedures must be in place to ensure satisfactory control over all changes to equipment, software or procedural documentation.

5.7.3. Incident Management Procedure

Incident management responsibilities and procedures must be clearly defined and documented to ensure a prompt, effective and orderly response to security incidents.

5.7.4. Segregation of Duties

Whenever appropriate, Astragraphia must implement segregation of duties to minimize the risk of intentional or unintentional misuse or misuse of Astragraphia's systems. Where this is not possible, other controls such as activity monitoring, audit trails, and management oversight should be considered.

5.7.5. Segregation of Development and Operational Facilities

As far as possible, Astragraphia should separate development from operational facilities and establish a formal process for moving software and/or hardware from one environment to another (both directions). The same environment must exist between development and testing. A stable test environment must be established to ensure that changes cannot be made to the test version of the software.

5.7.6. Protection Against Malicious Software

Software and related controls must be implemented in all Astragraphia systems to prevent and detect the introduction of malicious software. The introduction of malicious software such as computer viruses, network worm programs and Trojan horses can cause serious damage to networks, workstations and business data. Users should be aware of the dangers of unauthorized or malicious software. Astragraphia must implement controls to detect and prevent computer viruses from being introduced into the Astragraphia environment.

5.7.7. Network Management

Astragraphia must implement various network controls to maintain security on the internal network to make it reliable and protect services and connected networks. These controls must prevent unauthorized access to and use of Astragraphia's private network.

5.7.8. Internet Security & Acceptable Usage

- When employees connect to the Internet using "ag-it.com" or other Astragraphia designations, it should be for Astragraphia's business activities. Astragraphia's equipment, systems, facilities and equipment must be used only to carry out Astragraphia's business or for purposes authorized by management. The following is not a complete list, and only provides examples of behavior that may result in disciplinary action. In particular, the internet should not be used for personal use or benefit,
- To represent yourself as someone else (ie, "spoofing"),
- To ask Astragraphia employees to do something for other than business interests,
- To copy or transmit third party information without permission,
- To express personal opinions regarding vendors, suppliers, etc.,
- Provide information about, or list, Astragaphia employees to others,
- Untuk permohonan komersial kegiatan bisnis non-Astragraphia,
- For commercial applications for non-Astragraphia business activities,
- Interfering with the operation of the Internet gateway, for unauthorized attempts to break into a computing system whether including Astragraphia or any other organization (ie, cracking or hacking),
- To send messages that threaten or in any way harass another person,
- For theft or unauthorized copying of electronic files,
- To post sensitive Astragraphia information to unauthorized personnel,
- To download or upload information whose content could have legal consequences or reflect negatively on Astragraphia's reputation - including material relating to racial, sexual or religious statements; material with offensive language, graphics or images; or material prohibited by law,
- For "sniffing" (ie, monitoring network traffic), unless authorized to do so as part of their job responsibilities.

5.7.9. Extermal Internet Connections

Dial-up access to the Internet is prohibited from devices connected to any part of the Astragraphia network. This includes accounts with third-party Internet service providers. Users will not use an Astragraphia Internet account to establish connections with these third-party services, unless authorized to do so by Astragraphia management and the Information Security Manager.

Attempting to connect to the Internet from a firewall using any type of remote log-in or dial up service can compromise the integrity and security of the firewall.

5.7.10. **Connection to Third Party Networks**

Astragraphia private network connections to third party private networks must have business documents documented and approved by the Dept. ITSS Head and Information Security Manager. A risk analysis must be carried out to ensure that connection to a third-party network will not compromise Astragraphia's private network.

5.7.11. **E-Mail Security**

The electronic mail system is usually used for Astragraphia's business activities. Astragraphia maintains an electronic mail (e-mail) system for business use by employees and other authorized persons. Use of this system must comply with this policy and other Astragraphia standards and procedures regarding the use, distribution and disclosure of Astragraphia and other third-party proprietary information. The use of Astragraphia's electronic mail system can be monitored at random to comply with this policy.

Under normal circumstances, electronic mail/data is considered confidential between the sender and the recipient. Neither the sender nor the recipient may disclose the electronic mail/data to third parties at their sole discretion. Astragraphia's third party proprietary information may not be disclosed to individuals or organizations that are not Astragraphia without the knowledge and consent of the Information Owner. In some circumstances, at management's direction, it may be necessary for the Information Security Manager to access electronic mail/individual data in the investigation of suspected security incidents, or other special circumstances. Employees should not expect privacy when using Astragraphia's electronic mail system.

5.8. **Access Control**

The integrity, confidentiality and availability of Astragraphia's information assets will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, risk of loss or compromise and ease of recovery of these assets.

The Information Owner is responsible for determining who should have access to protected resources within their jurisdiction, and what access privileges they will have (read, update, etc.). These access rights must be granted according to the user's job responsibilities.

5.8.1. **User Registration and Access Management**

A formal user registration and de-registration (termination) process must be established and documented for all Astragraphia multi-user systems and services. This process is to prevent unauthorized access to Astragraphia information.

5.8.2. **User Password Management**

A persistent password is a common means of authenticating a user's identity to access information systems or services. Password standards must be developed and implemented to ensure that all authorized persons accessing Astragraphia's resources follow proven password management practices. These cipher rules should be mandated by system controls whenever possible. These password best practices include but are not limited to:

- Do not write passwords,
- Use passwords that are not easily guessed or subject to disclosure via dictionary attacks,
- Keep passwords confidential - do not share individual passwords with other users,
- Change passwords periodically,
- Change temporary password on first logon,
- Do not include passwords in any automatic logon process, for example stored in macros or function keys, or in Application codes.

5.8.3. Network Access Control

Access to Astragraphia's trusted internal network must require all authorized users to authenticate themselves through the use of individual user IDs and authentication mechanisms, for example, passwords, tokens or smart cards, or digital certificates. Network controls must be developed and implemented that ensure that authorized users can only access network resources and services necessary to perform their job responsibilities.

5.8.4. User Authentication for External Connections (Remote Access Control)

Individual accountability must be maintained when Astragraphia resources are accessed remotely. In order to maintain the highest standards of information security, Astragraphia requires that individual liability be maintained at all times, including during remote access. For the purposes of this policy, "remote access" is defined as incoming access to the Astragraphia network from outside the Astragraphia private and trusted network. This includes, but is not limited to:

- Calling from another location via a public line by an employee member or other authorized person;
- Connecting third party networks via dial or other temporary access technology to the Astragraphia network.

5.8.5. Network Segregation

When the Astragraphia network is connected to another network, controls must be exercised to prevent users from other connected networks from accessing sensitive areas, namely Astragraphia's private network. Router access control lists or other technologies must be implemented to control access to secure resources on a trusted Astragraphia network.

5.8.6. Operating System Access Control

Access to operating system code, services and commands should be restricted to those people who are necessary for the normal performance of their job responsibilities. All individuals (system programmers, database administrators, network administrators, etc.) must have a unique user ID for personal and sole use so that activity can be traced to the responsible person. The user ID should not give any indication of the privilege level of the user, e.g., supervisor, manager, administrator.

In certain circumstances, where there is a clear business advantage, the use of a shared user ID for a specific group of users or jobs may be used. Dept. approval. The ITSS head must be documented in these cases. Additional controls can be implemented to ensure accountability.

5.8.7. Application Access Control

Access to the system and application business should be limited to people who have a business need to access the application or system and such work is part of their job responsibilities. Access to source code on systems and applications must be limited to employees who have the duties of support only, and such access must be limited so that support employees can only access systems and applications for which they are authorized and responsible.

5.9. System Development and Maintenance

Software applications are developed or acquired to provide economic solutions to business problems. To ensure security is built into information systems, all security requirements must be identified at the project requirements stage and justified, approved and documented as part of the overall business case for the information system.

Security requirements and controls must reflect the business value of the information assets involved, and the potential business damage that may result from the failure or lack of security measures. The framework for analyzing security requirements and identifying controls to address them is linked to threat assessment and risk management.

5.9.1. Changes Management Procedure

To minimize the possibility of information system corruption, strict monitoring of changes in information systems must be implemented. Formal change control procedures should be in place. They must ensure that security and control procedures are not compromised, that support employees are given access only to those parts of the system necessary to perform their work, and that formal approval and approval processes for changes are in place. These change control procedures should be applied to business applications as well as system software used to maintain operating systems, network software, hardware changes, and so on.

5.9.2. Management Vulnerabilities

Potential technical vulnerabilities must be identified and addressed by the IT team. Vulnerability management techniques should address vulnerability monitoring, vulnerability risk assessment, locating and tracking assets. A timeline should be defined in response to technical vulnerability notices. Procedures should be established to classify the level of action taken as technical vulnerabilities arise in relation to change handling procedures or incident handling procedures.

The risks associated with installing the Patch should be assessed. Patches must be tested before installing. If Patch is not available, then other controls should be considered:

a. Change the service associated with the vulnerability.
b. Add access control.
c. Added monitoring to detect and prevent attacks.
d. Raise awareness of vulnerability.

Logs should be taken for all actions related to vulnerability fixing and/or patching and reviewed regularly. Appropriate technology should be used to assess technical vulnerabilities and should be audited annually.

5.10. Disaster Recovery Planing

The disaster recovery function for the information technology (IT) component should be performed by the Service Management organization. Responsible parties in this area should seek input from business processes and information owners regarding their recovery requirements for information technology in the line of business to ensure disruption to normal business operations is minimized.

5.11. Complience

5.11.1. Intellectual Property Rights

Appropriate procedures must be in place to ensure compliance with legal restrictions on the use of copyrighted material, or material that may have design or trademark rights. Proprietary software products are generally provided with a license agreement that limits the use of the product to a specific machine or number of users. Controls must be in place to ensure all aspects of the license agreement are met and can be audited. Copyright infringement can lead to legal action that may involve criminal proceedings.

5.11.2. Prevention of Misuse of Information Technology Resources

Information technology resources and data processed by these resources are provided for Astragraphia's business purposes. Management should allow its use. Any use of IT facilities for non-business or unauthorized purposes, without management approval, shall be considered as abuse of Astragraphia facilities.

5.11.3. **Compliance with Security Policy**
Managers must ensure that all security processes and procedures within their area of responsibility are followed. In addition, all business units at Astragraphia must be considered for regular review to ensure compliance with security policies and standards.

5.12. **Socialization**
This policy is periodically disseminated to all Astragraphia employees and external parties.

5.13. **Closing**
This policy will be adjusted if deemed necessary by taking into account the provisions of the laws and regulations in force in Indonesia.

6. Reference

6.1. NIST
6.2. ISO 27001
6.3. Law Number 11 of 2008 concerning Information and Electronic Transactions and amendments thereto ("UU ITE");
6.4. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data and Electronic Transactions ("Permen Perlindungan Data Pribadi”).
6.5. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (“PP PSTE”).

7. Related Documents

None