Information Security Policy

1. Purpose

The purpose of this Information Security Guidelines is to protect information assets, IT systems and networks managed by the company's IT organizational units to avoid adverse impacts on business, operations and reputation as a result of failures in the aspects of:

1.1 Confidentiality: in the context that access or dissemination of information is without clear authority.

1.2 Integrity: in the context of the accuracy, completeness of information and resistance to unauthorized modification or destruction.

1.3 Availability: in the context of the continuity of business processes and their recovery in the event of a breakdown/damage.

2. Scope

This policy applies to all Great Giant Pineapple business units.

3. Information Security Policy

3.1. Management Instructions

The company's information security policy must be established, approved by executive management, published and communicated to all employees and relevant external parties.

3.2. Reviewing

The information security policy should be reviewed periodically (at least annually) or when significant changes occur to ensure continued suitability, adequacy and effectiveness. This review aims to Continuously improving information security systems.

3.3 Ensuring Integrity and Protection of Data

The company are committed to safeguarding the integrity and security of all data. Access to sensitive information is restricted to authorized personnel, with robust security measures in place to prevent unauthorized access, alteration, or loss. We ensure compliance with relevant laws and regularly update our practices to address emerging threats, promoting transparency, accountability, and confidentiality in all data handling.

3.4 Monitoring and Responding to Information Security Threats

The company is dedicated to continuously monitoring information systems for potential security threats. The company utilize advanced tools and techniques to detect vulnerabilities and unauthorized activities in real-time. In the event of a security threat, we have a defined response protocol to quickly mitigate risks, minimize impact, and restore normal operations. Regular security audits and employee training ensure that we stay proactive in identifying and addressing evolving security challenges.

3.5 Establishing individual responsibilities for information security for the entire workforce

Each member of the company workforce is responsible for safeguarding the organization's information assets. All employees, contractors, and third-party personnel must adhere to established information security protocols, including data protection, secure access practices, and reporting potential security incidents. Regular training and awareness programs will be provided to ensure everyone understands their specific role in maintaining a secure environment. Failure to comply with these responsibilities may result in disciplinary actions to protect the integrity of the company information systems.

3.6 Establishing information security requirements for third parties (e.g. suppliers)

The company requires all third parties, including suppliers and contractors, to adhere to strict information security standards to protect our data and systems. Third parties must implement security measures that meet or exceed our own policies, including secure data handling, encryption, access controls, and compliance with relevant laws and regulations.

4. Information Security Organization

4.1. Information Security Organization

4.1.1. Employers must identify the information security responsibilities that apply to employees and include them in job descriptions, terms and conditions of employment.

4.1.2. The company must define resources and develop adequate organization for its information security activities.

5. Contact with Authorities and Special Groups

5.2.1. The company should have contact with authorities dealing with information security incidents.

5.2.2. The company's IT security personnel should maintain appropriate contact with specialist forums and professional associations in the field of information security.
5.2.2. Reporting information security incidents to the Indonesian government via the BSSN (Badan Siber & Sandi Negara), email address: pusopskamsinas@bssn.go.id

6. IT Asset Management, Classification and Protection of Information

6.1. Asset Inventory and Liability

6.1.1. A list of information assets should be created and maintained by a work unit responsible for all important information assets.

6.1.2. Each asset must have a defined owner/responsible person. Although responsibility for security measures can be delegated to specific individuals, accountability (responsibility) remains with the owner of the asset.

6.2. Asset Return

6.2.1. All employees and users of external parties must return all company assets that are under their responsibility in the event of termination of employment, termination of contracts or agreements.

6.2.2. The termination process should be formalized to ensure the return of all physical and electronic assets belonging to the company previously allocated to the personnel concerned.

6.3. Information Disposal

6.3.1. If the equipment/devices containing the storage media are permanently destroyed or are to be reused, all data and software must be deleted and physically destroyed.

6.3.2. If the equipment/device containing the storage media is no longer in use, it must be permanently destroyed/physically destroyed.

6.3.3 If the equipment/device containing the storage media is to be reused, all data and software must be deleted. Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data.

6.4. Removable Media Management

6.4.1. The company must have procedures governing the handling of removable media according to the classification scheme adopted by the company.

6.4.1. Companies must protect physical media during transit and in off-site storage media from unauthorized access, misuse, or damage when the media is outside the boundaries of the company's physical location.

7. Acceptable Use of IT Asset

7.1. Acceptable Use Policy

7.1.1. Policies for the use of information, assets related to information and acceptable information processing facilities must be identified, documented and implemented, including rules for the use of email, internet and social media.

7.2. Email Acceptable Use

7.2.1. Each employee should be responsible for the content of his or her own email.

7.2.2. Email accounts are created and assigned to authorized individuals and may not be used as shared accounts.

7.2.3. Individuals who access the company's email services may not use or access another individual's email account or send or receive messages with another individual's account.

7.2.4. Company email systems may not be used to create or distribute disturbing or offensive messages, including offensive comments about race, gender, disability, age, sexual orientation, pornography, religious beliefs and practices, political beliefs, or national origin.

8. Access Control

8.1. User Access Management

8.1.1. All users must have their own individual user account, for which they are fully responsible for the user account.

8.1.2. Formal user access control procedures must be documented, implemented and kept up to date to ensure authorized user access and to prevent unauthorized access.

8.1.3. Companies must implement a user access provisioning process to assign or revoke access rights for all types of users to all IT systems and services.

8.1.4. User access rights should be reviewed periodically (at least annually) and where changes occur to ensure that appropriate rights are still allocated.

8.1.5. Access rights for all employees and external parties must be removed upon termination of the contract or agreement.

8.1.6. Employees are only entitled to access the IT system according to the access rights that have been granted. If they access the system outside their authority will be subjected to diciplinary action / warning letter from referring to HR regualtion.

8.2. Privilege Management

8.2.1. Privilege accounts must be controlled by restricting access to only authorized users.

8.3. Secret Authentication

8.3.1. The provision of secret authentication information must be controlled through a formal management process.

8.4. Remote Access Control

8.4.1. Companies must ensure that remote access to information systems and networks is adequately controlled.

8.4.2. Remote access rights must be formally approved, on the basis of verified business requirements.

8.4.3. Remote access should not be granted by default to all account holders on the company's main network.

8.4.4. Remote access to information systems and network resources (switches, routers, computers, etc.) is only permitted through secure, authenticated and centrally managed access methods.

8.4.4.1. For teleworking and mobile working, access to company information, networks and applications (including email) can be attained via the secure network (Virtual Private Network).

8.4.4.2. Connection to the network should only be attempted using the domain login and password credentials.

8.5. Password Management

8.5.1. A password policy must be in place to manage all user accounts and administrative accounts of IT systems. Password must be at least 10 characters, meet complexity & lifetime of 90 calendar days.

8.5.2. Two factor authentications such as one time password, smart cards, or challenge response tokens can be used to protect all sensitive information including administrative functions and remote access to assets including network.

9. Desktop and Mobile Device Security

9.1. Desktop and Mobile Devices

9.1.1. Companies must develop policies and procedures governing the use of desktop and mobile devices such as notebooks, tablets and mobile phones.

9.1.2. Desktop and mobile devices connected to, or transacting data with the company's main network, must have anti-malware protection installed.

9.1.3. Desktop and mobile devices should only be installed with officially licensed applications.

9.1.4. Desktops and mobile devices must be configured with a secure password in accordance with the company's password policy.

9.1.5. Desktops and mobile devices used for work in an office environment are only allowed to use company-owned devices.

10. IT Operation

10.1. Operational and Maintenance Procedure

10.1.1. Required operational and maintenance procedures must be documented, updated and accessible to those who need them.

10.2. Change Management

10.2.1. Change management procedures to the organization, business processes, systems and information processing facilities must be controlled.

10.3. Capacity Planning

10.3.1. The use of IT system resources and services that support the company's business processes must be monitored and future capacity projections must be made so as to maintain the availability and performance of IT systems and services.

10.4. System Environment Separation

10.4.1. The testing environment should be separated from the development and production environments to reduce the risk of unauthorized access or alteration.

10.5. Protection Against Malware

10.5.1. Companies must implement protection against malware (such as viruses, trojans, botnets, etc.) on information systems and network devices.
10.5.2. The anti-malware software is capable of detecting all known forms of malware, including viruses, Trojans, worms, spyware, adware, and rootkits.
10.5.3. The anti-malware software is installed on all information systems and devices.

10.6. Backup dan Restore

10.6.1. Backup procedures should be in place to copy all important data stored on company network servers. The backup process is run at least once a week, or more frequently, based on the sensitivity of the data.
10.6.2. Backup copies of company information and software should be made and tested for recovery (restore) regularly (at least annually) in accordance with established policies.
10.6.3. Backups of data that are not stored on network servers should be the responsibility of the user.

11. Technical Penetration Testing dan Patch Management

11.1. Information System Configuration Standard

11.1.1. Companies must establish, document and implement secure configuration standards for all information systems.

11.2. Penetration Testing

11.2.1. Information on information system and network vulnerabilities must be obtained periodically, the company's level of exposure to these vulnerabilities must be evaluated and addressed to address the associated risks.
11.2.2. Penetration Testing in IT systems at least once in two years.
11.2.3. Implementation of a methodology for penetration testing that includes the following:

11.2.3.1. Industry best practices for vulnerability management are updated (for example, the Open Web Application Security Project/OWASP Guide, SANS Common Weakness Enumeration/CWE Top 25, Community Emergency Response Team/CERT secure coding, etc.), the current best practices must be used for these requirements.

11.3. Patch Management

11.3.1. Security patches and other related security updates should always be implemented when available and approved, unless this creates a higher business risk.

11.3.2.Automatic operating system updates are implemented automatically for comprehensive protection including patch / security updates.

11.3.3. Systems that cannot be updated for any reason must be isolated from the main network or other security measures must be installed to protect vulnerable systems. All changes must be made in accordance with the requirements or procedures governing system changes.

President Director
PT Great Giant Pineapple

Tommy Wattimena