# KEBIJAKAN TATA KELOLA TEKNOLOGI INFORMASI

# POLICY OF INFORMATION TECHNOLOGY GOVERNANCE

**Edisi/Edition: 1 (Satu)/ 1 (One)**
**Berlaku sejak/Valid since : 20 Juli 2023/ July 20, 2023**

**KEBIJAKAN TATA KELOLA TEKNOLOGI INFORMASI**
**PT AUSTINDO NUSANTARA JAYA Tbk.**

## 1. TUJUAN

Dalam rangka penerapan prinsip Tata Kelola Perusahaan yang Baik (*Good Corporate Governance*) maka PT Austindo Nusantara Jaya Tbk. ("**Perseroan**") mengeluarkan kebijakan ini mengenai tata kelola teknologi informasi sesuai ketentuan yang berlaku.

Kebijakan Tata Kelola Teknologi Informasi ("**Kebijakan**") ini bertujuan untuk menjadi pedoman untuk memastikan tata kelola dan mitigasi risiko atas permasalahan teknologi informasi seperti gangguan, keamanan dunia maya dan pemulihan bencana dilakukan secara efektif dan sesuai dengan peraturan perundang-undangan yang berlaku.

## 2. RUANG LINGKUP

Kebijakan ini berlaku untuk Perseroan, seluruh anak perusahaan Perseroan dan karyawan Perseroan.

## 3. DASAR HUKUM

1) Undang-undang No. 40 Tahun 2007 tentang Perseroan Terbatas.

**POLICY OF INFORMATION TECHNOLOGY GOVERNANCE OF**
**PT AUSTINDO NUSANTARA JAYA Tbk.**

## 1. OBJECTIVE

In order to implement the principles of the Good Corporate Governance, PT Austindo Nusantara Jaya Tbk. (the "**Company**") issues this policy relating to information technology governance in accordance with applicable laws and regulations.

This policy regarding Information Technology Governance ("**Policy**") is a guideline to ensure governance and risk mitigation of information technology issues such as disruption, cyber security and disaster recovery are carried out effectively and in accordance with applicable laws and regulations.

## 2. SCOPE

This Policy is applicable to the Company, its subsidiaries and employees of the Company.

## 3. LEGAL BASIS

1) Law No. 40 of 2007 regarding Limited Liability Company.

**PT Austindo Nusantara Jaya Tbk.**
Menara BTPN Lantai 40
Jalan Dr. Ide Anak Agung Gde Agung Kav. 5.5 - 5.6
Kawasan Mega Kuningan, Jakarta 12950
**T** (62 21) 2965 1777 **F** (62 21) 2965 1788
**www.anj-group.com**

2) Anggaran Dasar Perseroan.

2) The Articles of Association of the Company.

## 4. TATA KELOLA TEKNOLOGI INFORMASI

1) *Disruption* dan *Cyber Security*

Perseroan telah memiliki beberapa kebijakan dalam pelaksanaan tata kelola teknologi informasi untuk menghindari dan/atau memitigasi risiko atas terjadinya gangguan (*disruption*) dan untuk sistem keamanan dunia maya (*cyber security*) Perseroan yaitu sebagai berikut:

a. Manual Kebijakan Penerapan Standar Konfigurasi dan Penerapan Keamanan Teknologi Informasi;

b. Manual Kebijakan Pembuatan dan Penggunaan Surel Perusahaan;
c. Manual Kebijakan Penggunaan Akses Internet;
d. Kebijakan Keamanan Informasi;

Perseroan melakukan implementasi terhadap kebijakan-kebijakan tersebut, yang dilakukan dengan cara sebagai berikut:

a. Membuat satuan kerja penyelenggara teknologi informasi untuk melakukan perencanaan, pengadaan, pengelolaan, penerapan dan

## 4. INFORMATION TECHNOLOGY GOVERNANCE

1) Disruption and Cyber Security

The Company has several policies in the implementation of information technology governance to avoid and/or mitigate the risk of disruption and for cyber security system of the Company, as follows:

a. The Policy Manual for the Implementation of Information Technology Security Configuration and Implementation Standards;
b. The Policy Manual for the Creation and Use of the Company Email;
c. The Policy Manual on the Use of Internet Access;
d. Information Security Policy;

The Company implements these policies, which are carried out in the following manners:

a. To establish an information technology work unit to plan, procure, manage, implement and supervise information, applications, hardware,

| | |
|---|---|
| pengawasan terhadap informasi, aplikasi, perangkat keras, perangkat lunak dan infrastruktur agar selalu memerhatikan risiko atas terjadinya gangguan (*disruption*) dan memitigasi risiko keamanan dunia maya (*cyber security*). | software and infrastructure so that it always observes the risk of disruption and mitigates cyber security risks. |
| b. Memantau perangkat jaringan, pemeliharaan sistem Perseroan, server penyimpanan data Perseroan, pembatasan akses internet, penerapan keamanan teknologi informasi dan penerapan cadangan data apabila terjadi keadaan darurat secara berkala oleh penyelenggara informasi teknologi. | b. Maintain the Company's systems, store data servers, limit internet access, implement information technology security and implement data backups in the event of an emergency regularly by information technology providers. |
| c. Melakukan sosialisasi dan/atau *awareness* kepada seluruh unit kerja dan/atau karyawan Perseroan atas pelaksanaan kebijakan pengelolaan teknologi informasi. | c. Conduct socialization and/or awareness to all work units and/or employees of the Company regarding the implementation of information technology management policies. |
| d. Mengirimkan *e-mail* sosialisasi dan/atau *awareness* kepada seluruh karyawan Perseroan. | d. Send socialization and/or awareness e-mails to all of employees of the Company. |
| e. Melakukan pembahasan terkait pengelolaan teknologi informasi di dalam Rapat Manajemen. | e. Conduct discussions related to the management of information technology in Management Meetings. |
| f. Mengintegrasikan sistem, aplikasi dan jaringan Perseroan agar meningkatkan efektivitas dan efisiensi operasional Perseroan dan bisnis Perseroan | f. Integrate the systems, applications and networks of the Company in order to increase the effectiveness and efficiency of the Company's operations |

yang mendukung pada keberlanjutan Perseroan.

g. Melakukan evaluasi secara berkala atas kebijakan-kebijakan pengelolaan teknologi informasi Perseroan agar dapat memenuhi kebutuhan Perseroan dan memitigasi risiko gangguan (*disruption*) dan/atau keamanan dunia maya (*cyber security*).

2) Pemulihan Keadaan Darurat dan/atau Bencana (*Disaster*)

Perseroan telah memiliki kebijakan atau *Standard Operation Procedure* (SOP) tentang Pemulihan Keadaan Darurat ICT yang mengacu pada Manual Kebijakan *Business Continuity Plan*. SOP Pemulihan Keadaan Darurat ICT mencakup prosedur penanganan dan pemulihan sistem baik infrastruktur, komunikasi dan aplikasi Perseroan jika terjadi keadaan darurat dan/atau bencana.

Perseroan melakukan implementasi terhadap kebijakan tersebut, yang dilakukan dengan cara sebagai berikut:

a. Membuat dan mengevaluasi rencana pemulihan bencana (*disaster recovery plan)* secara berlaka oleh penyelenggara teknologi informasi untuk mengatasi dampak bencana

and the Company's business that supports the Company's sustainability.

g. Conduct periodical evaluations of information technology management policies of the Company in order to meet the Company's needs and mitigate the risk of disruption and/or cyber security.

2) Emergency and/or Disaster Recovery

The Company has a policy or Standard Operation Procedure (SOP) regarding to ICT Emergency Recovery that refers to the Business Continuity Plan Policy Manual. The ICT Emergency Recovery SOP includes procedures for handling and restoring the Company's infrastructure, communication and application systems in the event of an emergency and/or disaster.

The Company implements the above policy, which is carried out in the following manners:

a. Draw up and evaluate disaster recovery plans regularly by information technology work unit to address the impact of disasters so as to ensure the

sehingga dapat menjamin kegiatan usaha dan operasional Perseroan.

b. Melakukan pengembangan rencana pemulihan bencana (*Disaster Recovery Plan*) baik dari sisi infrastruktur, komunikasi dan aplikasi untuk meminimalisir terjadinya kegagalan atau kerusakan.

c. Melakukan evaluasi dan pengujian secara berkala terhadap *Business Continuity Plan* (BCP) bersama antara penyelenggara teknologi informasi dan Departemen *Business Process*.

d. Membuat penyimpanan cadangan atas data, dokumen dan/atau informasi Perseroan jika terjadi bencana.

business and operational activities of the Company.

b. Develop a disaster recovery plan in terms of infrastructure, communication and applications to minimize the occurrence of failure or damage.

c. Conduct periodical evaluation and testing of the Business Continuity Plan (BCP) jointly with information technology work unit and the Business Process Department.

d. Create backup storage of data, documents and/or information of the Company in the event of a disaster.

**5. Lain-Lain**

Perseroan akan mengevaluasi Kebijakan ini setiap tahun agar sesuai dengan peraturan yang berlaku.

***

**5. Miscellaneous**

The Company shall review this Policy annually to conform to the prevailing regulations.

***