



*PT INDEXIM COALINDO*


# **SECURITY MANAGEMENT SYSTEM**

## **SISTEM MANAJEMEN PENGAMANAN**

DOC NO.XXX XXXX

# **CONFIDENTIAL**

## **(RAHASIA)**

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 2 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

## POLICY AND PROCEDURE AUTHORIZATION

### PREPARED BY:

NAME

SIGNATURE

POSITION

### REVIEWED BY:

NAME

SIGNATURE

POSITION

### APPROVED BY:


NAME

SIGNATURE

POSITION


This document is controlled Controlled Document.If using a print out of this document, please check the document status first to ensure that it is the latest version and complies with the controlled document procedure. If there is any newer version please dispose of the obsolete document or mark it as "obsolete". This document must not be reproduced or photocopied for use outside The Company without prior approval from the PT PT Indexim Coalindo

**CONFIDENTIAL**

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 3 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

### SUMMARY OF REVISION

Date	Ver.	Section	Description	Approval

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 4 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

## 1. Purpose

This manual is made to explain and carry out security management system in securing company's property, asset, and employees for the corporate business sustainability.

## 2. Scope

This manual is applied to all business processes, activities, and working sites of PT Indexim Coalindo

## 3. Reference

- Indonesian Police Regulation No.24, 2007 about Security Management System
- Indonesian Police Regulation No.24, 2010 regarding Security Business Provider
- TAPA (Transportation and Assest Protection Associations)
- ISO 27001 ISMS
- ISPS Code (international Ship and Port security)

## 4. Definition

Security Management System: is a Security Management Standard based on Indonesian Police Regulation No.24, 2007 which is purposed to support the organization in managing effectively the security management system elements to be embedded in other standard management requirements. This standard is also aimed to help the organization to achieve economic importance and security

## 1. Tujuan

Panduan ini dibuat untuk menjelaskan dan melaksanakan sistem manajemen keamanan dalam menjamin kemampuan untuk melindungi properti, asset dan karyawan perusahaan dalam upayanya untuk menjamin kelangsungan bisnis perusahaan.

## 2. Ruang Lingkup


Panduan di aplikasikan pada semua proses bisnis, aktifitas dan lokasi kerja di PT Indexim Coalindo

## 3. Referensi

- Peraturan Polisi No. 24 tahun 2007 tentang Sistem Manajemen Pengamanan
- Peraturan Polisi No. 24 tahun 2010 tentang BUJP
- TAPA (Transportation and Assest Protection Associations)
- ISO 27001 ISMS
- ISPS Code (international Ship and Port security)

## 4. Definisi

Sistem Manajemen Pengamanan: Standar manajemen pengamanan berdasarkan Perpol no.24 tahun 2007 ini dimaksudkan untuk membantu organisasi dalam mengelola secara efektif elemen-elemen sistem manajemen pengamanan yang dapat disatukan dengan persyaratan standar manajemen lainnya. Standar ini juga

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 5 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

goals. This standard is like other standards where it stands not as obstacles in trading nor duty changes to current valid regulations.

dapat membantu organisasi untuk mencapai sasaran pengamanan dan kepentingan ekonomi. Standar ini seperti standar lainnya tidak dimaksudkan untuk digunakan bukan sebagai penghambat atau merubah kewajiban terhadap peraturan

## 5. Procedure

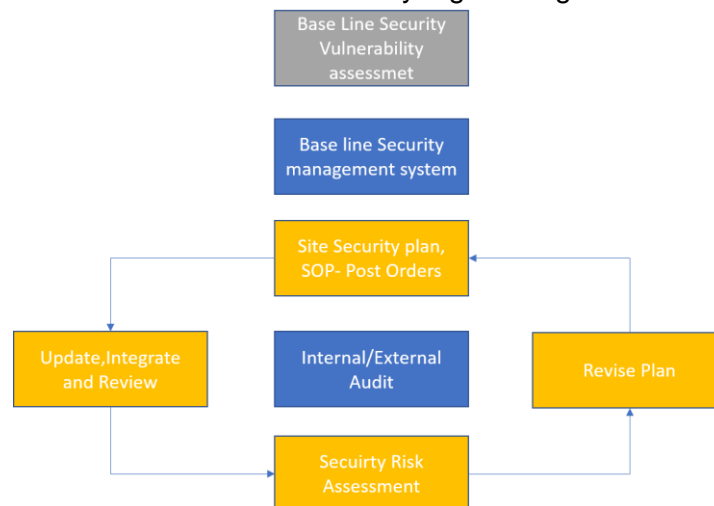
The following are PT INDEXIM COALINDO Policy documents related to Security Management System development and implementation process.

Conceptual design for Integrated Security Management system

## 5. Prosedur

Berikut ini merupakan dokumen Kebijakan PT INDEXIM COALINDO yang terkait sebagai dasar proses pengembangan dan pelaksanaan Sistem Manajemen Pengamanan.

Konsep Security management Sistem yang terintegrasi dan berkelanjutan



### Base line Security management system:


Using the output of the SVA, a SMS is developed to address the most significant risks and assess the security of the facility or asset

**Site Security plan** the baseline security site plan activities are implemented, the results are evaluated, and the necessary changes are made to ensure risks that might lead to system failures are controlled

### Sistem manajemen keamanan garis dasar:

Menggunakan output dari SVA (Security Vulnerability Assessment, SMS (Security Management System) dikembangkan untuk mengatasi risiko yang paling signifikan dan menilai keamanan fasilitas atau aset

**Rencana Keamanan** : rencana awal sistem keamanan diimplementasikan, hasilnya dievaluasi, dan perubahan

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 6 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

**Upgrade Integrate and Review:** After the initial stage, security plan has been performed, the facility will have improved and updated information about the security of the facility.

**Security Risk Assesment;** should be performed periodically to factor in recent operations, consider changes to the facility design, and to analyze the impact of any external changes that may have occurred since the last Assessment

yang diperlukan dibuat untuk memastikan risiko yang dapat menyebabkan kegagalan sistem dikendalikan

**Tingkatkan Integrasi dan Tinjauan:** Setelah tahap awal, rencana keamanan dilakukan, Manajemen keamanan akan meningkatkan dan memperbarui informasi tentang keamanan fasilitas.

**Penilaian Risiko Keamanan;** harus dilakukan secara berkala untuk memperhitungkan operasi keamanan terbaru, mempertimbangkan perubahan pada desain fasilitas, dan untuk menganalisis dampak dari setiap perubahan eksternal yang mungkin terjadi sejak Penilaian terakhir

## 5.1 Responsibilities

5.1.1 The Board of Directors shall responsible to:

- Ensure the availability of enough resources in managing security aspects
- Review and validate all policies, purposes, and security management system targets in Corporate.
- Assign to Project Manager or related department to plan, implement, monitor, and review Security Plan and Action Plan to guarantee achievable purposes and goals.

5.1.2 Department Manager shall responsible to:

- Carry out duties and responsibilities with regards to detail job and position function in each department's business process according to its Security Plan related to the function of implementing security management system.
- Identify training needs for all levels and

## 5.1 Tanggung Jawab


5.1.1 Dewan Direksi bertanggung jawab untuk :

- Menjamin ketersediaan sumberdaya yang diperlukan secara memadai dalam pengendalian terhadap aspek keamanan
- meninjau ulang dan mengesahkan kebijakan, tujuan dan target sistem pengamanan secara keseluruhan di Corporate.

- menunjuk dan memberikan tanggung jawab kepada Manajer Proyek atau Departemen terkait untuk merencanakan, melaksanakan, memantau dan melakukan tinjauan atas Security plan dan Action Plan untuk menjamin bahwa tujuan dan sasaran dapat dicapai.

5.1.2 Manager Departemen bertanggung jawab untuk :

- Melaksanakan tugas dan tanggung jawab sesuai dengan rincian tugas dan fungsi jabatan pada business proses

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 7 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

cross functional team to meet the need of security management system implementation

- Communicate to all levels in each department about requirements, and security management system implementation.
- Coordinate and communicate regularly for implementation OBVITNAS

5.1.3 All employees take the responsibility to:

- Take care and participate in any program and maintenance of the security management system implementation according to given responsibility and authority.

5.2 The policy on PT Indexim Coalindo Security Management System should be established by Top Management and covers:

- Appropriate culture and level of threat risks from organization;
- The commitment to sustainable improvement on security management and organization's performance and legal requirements accomplishment; or other requirements.
- The commitment to involve community as security instruments;
- Communicating it to all employees as personal responsibility;
- Regular review to ensure its balance and properness for the organization.

departemen masing-masing sesuai dengan rencana pengamanan dalam keterkaitannya menjalankan fungsi dalam sistem manajemen pengamanan.


- Mengidentifikasi kebutuhan training untuk seluruh jajaran dan cross functional team terhadap keperluan pelaksanaan sistem manajemen pengamanan
- Mengkomunikasikan kepada seluruh jajaran dalam area departemennya mengenai persyaratan, dan perkembangan pelaksanaan sistem manajemen pengamanan.
- Melakukan koordinasi dan komunikasi rutin untuk implementasi OBVITNAS ke jajaran Polisi dan atau Militer

5.1.3 Seluruh Karyawan bertanggung jawab untuk :

- Peduli dan ikut serta dalam program maupun pemeliharaan pelaksanaan sistem manajemen pengamanan sesuai dengan tanggung jawab dan kewenangan yang diberikan.

5.2 Kebijakan terhadap PT INDEXIM COALINDO Sistem Manajemen Pengamanan harus ditetapkan oleh Manajemen Puncak dengan mencakup kepada:

- Kesesuaian dengan budaya setempat dan skala dari risiko ancaman dari organisasi;
- Mencakup komitmen untuk peningkatan berkelanjutan dalam manajemen pengamanan dan kinerja organisasi serta upaya pemenuhan persyaratan perundangan; maupun persyaratan lainnya.
- Mencakup komitmen untuk melibatkan komunitas sebagai instrumen pengamanan;
- Dikomunikasikan kepada seluruh karyawan dan menjadi tanggung

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 8 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

**5.3** The scope of PT INDEXIM COALINDO's Security Management System covers all activities and business processes in relation with the plan and implementation to reduce risk potential on:

- Strategic
- Technical
- Operational
- Commercial, and
- Financial Control

#### **5.4 Risk Management on Corporate Business**

**5.4.1** Systematic approach to identify the capability of securing company's property, asset, and employees in order to guarantee company's sustainable business through determined risk measurement method. Where defined risk profile is utilized as a basic to make functional plan in company's business processes and will be periodically reviewed, by considering the following:

- Industrial characteristic,
- Geographic,
- Information Technology Development
- Required Statistic Data; or comparable data;
- Intelligent information from local authorities, province or state of potential risk on business sustainability;
- World's industrial information on security level tendency
- General economic condition;

jawab secara personal;

- Ditinjau ulang secara berkala untuk memastikan kesesuaian dan kelayakannya bagi organisasi.

**5.3** Ruang lingkup PT INDEXIM COALINDO Sistem Manajemen Pengamanan meliputi seluruh aktifitas dari bisnis proses yang terkait terhadap perencanaan dan pelaksanaan mengurangi potensi resiko :


- Strategis
- Teknis
- Operational
- Komersial, dan
- Finansial Kontrol

#### **5.4 Risk Management on Corporate Business**

**5.4.1** Pendekatan secara sistematis untuk mengidentifikasi risiko terhadap kemampuan untuk melindungi property, asset dan karyawan perusahaan dalam upayanya untuk menjamin kelangsungan bisnis perusahaan melalui metode penilaian resiko yang telah ditentukan. Dimana profil resiko yang diperoleh digunakan sebagai dasar dalam melakukan perencanaan fungsi dalam bisnis proses perusahaan yang ditinjau secara periodik, dengan mempertimbangkan hal berikut tanpa terbatas pada:

- karakteristik industri,
- letak geografis,
- perkembangan teknologi informasi
- Data statistik yang diperlukan; atau data yang dapat diperbandingkan;
- Informasi intelijen dari pemerintah daerah, provinsi atau pusat tentang potensi ancaman terhadap kelangsungan usaha;
- Informasi dunia industri tentang kecenderungan tingkat keamanan;
- Kondisi ekonomi secara umum;



	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 9 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

5.4.2 In a situation where a risk measurement on certain site is required to support company's operation, there will be risk evaluation done as a specific program outside risk management on business by considering time, support, and appropriate resources.

## 5.5 Security Management System Purpose and Goals

5.5.1 In every functional plan, there should be purposes and goals established as performance key indicators that match with each business process characteristic in doing risk mitigation that will impact to the company's business capability. When determining purpose and goals, consider the following:

- Fulfill requirements on law regulations and other requirements,,
- Sustainable improvement;
- Decision on technology,
- Business and operation requirements,
- Descriptions from related parties;
- Risk level

5.5.2 In relation with Purpose and Goals to other involved parties in the implementation of PT INDEXIM COALINDO's security management, it is described in a contractual form as annual Quality Objectives (KPI/SLA) which will be periodically evaluated by PT INDEXIM COALINDO and Security Provider Management.

## 5.6 Physical Facility and Ground Rules

5.6.1 Control Access:

Use "layers" of security appropriate to the threat level to prevent unauthorized persons from having access to critical

5.4.2 Pada situasi dimana diperlukan adanya penilaian resiko terhadap area tertentu untuk mendukung operasi perusahaan, maka akan dilakukan penilaian resiko sebagai program spesifik tanpa dimasukkan dalam manajemen resiko terhadap bisnis dengan mempertimbangkan waktu, dukungan dan kesesuaian sumber daya

## 5.5 Tujuan dan Sasaran Manajemen Pengamanan

5.5.1 Pada setiap perencanaan fungsi harus ditentukan tujuan dan sasaran yang dijadikan sebagai indikator kunci kinerja sesuai dengan karakteristik masing-masing bisnis proses dalam melakukan mitigasi resiko yang berdampak pada kemampuan bisnis perusahaan. Dalam menentukan Tujuan dan Sasaran harus mempertimbangkan pada :


- pemenuhan persyaratan peraturan perundang-undangan dan persyaratan lainnya,
- perbaikan berkelanjutan;
- pilihan atas teknologi,
- persyaratan operasi dan bisnis,
- serta gambaran dari pihak-pihak terkait;
- Tingkat resiko

5.5.2 Terkait dengan Sasaran dan Tujuan kepada pihak lain yang terlibat dalam pelaksanaan pengamanan fasilitas PT INDEXIM COALINDO dijabarkan dalam bentuk kontraktual sebagai Sasaran Mutu tahunan yang dievaluasi secara periodik oleh PT INDEXIM COALINDO dan BUJP Manajemen.

## 5.6 Fasilitas Fisik dan Aturan dasar

5.6.1 Kontrol Akses:

Penggunaan sistem "lapisan/ring" keamanan yang sesuai dengan tingkat ancaman untuk mencegah orang yang

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 10 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

assets or areas of the facility, as identified in the risk assessment.

A "layered" security approach to control access to the facility and its critical assets involves implementing a combination of physical and operational measures.

5.6.2 Physical security options may include, but are not limited to, one or a combination of the following options:

Installing security lighting in high-risk or dimly lit areas. Consider using high-low ballast lighting, in which high-beam light is activated by physical movement of intruders in the area(s) subject to surveillance.

Conducting periodic walk-arounds by company personnel of the facility to all Restricted Area, Plant loading/unloading areas.

Conducting drive-by surveillance patrols by local law-enforcement on a regular, but unpredictable, basis.

Installing electronic security devices, such as door alarms (*e.g., horns, bells, etc.*), motion-detection devices and alarms monitored by an off-site security system or contractor.

Installing appropriate signage for:

- "No trespassing."
- "Private property."
- "Visitor Parking."
- "All visitors must check in with front office."
- "All visitors must be escorted."
- "No vehicles beyond this point."
- "Patrolled" (*if appropriate*).
- "Closed-Circuit TV surveillance" (*if appropriate*).
- ISPS Level
- OBVITNAS notification Board

tidak berwenang dari memiliki akses ke aset penting atau area fasilitas, seperti yang diidentifikasi dalam penilaian risiko.

Pendekatan keamanan "berlapis" untuk mengendalikan akses ke fasilitas dan aset kritisnya melibatkan penerapan kombinasi tindakan fisik dan operasional.

5.6.2 Opsi keamanan fisik dapat mencakup, tetapi tidak terbatas pada, satu atau kombinasi dari opsi berikut:

Menempatkan lampu keamanan di area berisiko tinggi atau remang-remang. Pertimbangkan untuk menggunakan pencahayaan ballast tinggi-rendah, di mana cahaya sinar tinggi diaktifkan oleh gerakan fisik pengganggu di area yang harus diawasi apabila memungkinkan.


Melakukan walk-around/inspeksi secara berkala oleh personel perusahaan dari fasilitas ke semua Area Terbatas, area pemuatan / pembongkaran dan produksi.

Melakukan patroli pengawasan drive-by oleh penegak hukum setempat secara teratur yang tidak dapat diprediksi.

Memasang perangkat keamanan elektronik, seperti alarm pintu (*mis., Klakson, bel, dll.*), Perangkat pendeteksi gerakan dan alarm yang dipantau oleh sistem keamanan luar atau kontraktor.

Memasang signage yang sesuai untuk:

- "Dilarang melintas."
- "Milik pribadi."
- "Parkir Pengunjung."
- "Semua pengunjung harus check-in dengan front office."
- "Semua pengunjung harus dikawal."
- "Tidak ada kendaraan di luar titik

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 11 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

Installing video surveillance.

Retaining guard service from contract security firms.

Installing physical barriers, such as virtual or visible perimeter fencing and locked gates.

Enrolling in a local business or community "crime- watcher's" program.

#### Operational measures include:

Designating specific access points to the facility, and posting appropriate signage.

Screening persons and vehicles prior to entry.

Requiring acceptable identification, such as a valid driver's license or government issued identification card, for individuals prior to entry.

Designating restricted areas of the facility and grounds, and posting appropriate signage, to prevent or deter unauthorized access. Consider the presence of unauthorized persons in restricted areas to be a breach of security that requires immediate notification of management.

Limiting employee access to critical areas or assets of a facility based upon their job functions.

Updating employee shift rosters (e.g., *noting absences, replacements, etc.*) for supervisors at the start of each shift so they know who is expected to be on

- ini."
- "Patroli" (jika perlu).
- "Pengawasan TV Sirkuit Tertutup" (jika sesuai).
- ISPS Security Level
- OBVITNAS notifikasi

Menggunakan pengawasan CCTV.

Menggunakan layanan pengamanan dari perusahaan keamanan.

Memasang penghalang fisik, seperti pagar pembatas virtual atau terlihat dan gerbang selalu dalam kondisi terkunci.

Mengikut sertakan perusahaan dalam komunitas "crime watcher" apabila tersedia dilokasi tersebut.

#### Langkah-langkah operasional meliputi:


Menentukan titik akses spesifik masuk dan keluar ke fasilitas, dan memasang signage yang sesuai.

Menyaring orang dan kendaraan sebelum masuk.

Diperlukan identifikasi yang dapat diterima, seperti SIM yang valid atau kartu identitas yang dikeluarkan pemerintah, untuk individu sebelum masuk.

Menetapkan area terbatas pada fasilitas dan lahan, dan memasang papan nama yang sesuai, untuk mencegah atau menghalangi akses tidak sah. Pertimbangkan keberadaan orang yang tidak berwenang di area terlarang sebagai pelanggaran keamanan yang membutuhkan pemberitahuan segera dari manajemen.

Membatasi akses karyawan ke area penting atau aset fasilitas berdasarkan fungsi pekerjaan mereka.

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 12 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

site.

Imposing increasingly stringent measures for accessing critical areas or assets of the facility.

#### 5.6.3 Establish Procedures for Access to Facility and Grounds by Visitors, Outside Contractors, Vendors:

Limit access of the facility and mining area to non-company personnel, such as outside contractors, vendors, truck drivers and others.

- Designate specific areas for parking for visitors, outside contractors and vendors.
- Require visitors to check-in with a designated company representative upon arrival; consider posting signs informing visitors of where to report in.
- Maintain a visitor's log book that requires sign-in upon entry, along with required identification, company name and purpose of the visit, and sign- out when departing.
- Consider using name badges/tags, identification cards or other means (such as a special hat, etc.) to identify visitors.
- Restrict access to storage area. Do not allow visitors, including delivery personnel, contractors and vendors, to wander the premises.
- Consider adopting policies that require visitors to be accompanied/escorted by a company employee before being granted access.


Memperbarui daftar nama shift karyawan (mis., Mencatat absen, penggantian, dll.) Untuk penyelia pada awal setiap shift sehingga mereka tahu siapa yang diharapkan berada di lokasi.

Menerapkan tindakan yang semakin ketat untuk mengakses area kritis atau aset fasilitas.

#### 5.6.3 Menetapkan Prosedur untuk Akses ke Fasilitas dan area tambang oleh Pengunjung, Kontraktor Luar, Vendor:

Batasi akses fasilitas ke personel non-perusahaan, kontraktor luar, vendor, pengemudi truk , dan lainnya.

- Tentukan area khusus untuk parkir bagi pengunjung, kontraktor luar dan vendor.
- Mewajibkan pengunjung untuk check-in dengan perwakilan perusahaan yang ditunjuk pada saat kedatangan; pertimbangkan memposting tanda yang menginformasikan pengunjung tempat melapor.
- Menyimpan buku catatan pengunjung yang memerlukan masuk saat masuk, bersama dengan identifikasi yang diperlukan, nama perusahaan dan tujuan kunjungan, dan keluar saat berangkat.
- Pertimbangkan untuk menggunakan badge nama / tanda, kartu identifikasi atau cara lain (seperti topi khusus, dll.) Untuk mengidentifikasi pengunjung.
- Batasi akses ke penyimpanan hasil tambang. Jangan izinkan pengunjung, termasuk petugas pengiriman, kontraktor, dan vendor, berkeliaran di tempat itu.
- Pertimbangkan untuk mengadopsi kebijakan yang mengharuskan pengunjung ditemani / dikawal oleh karyawan perusahaan sebelum

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 13 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

diberikan akses

#### 5.6.4 Secure the Facility / Operations activity:

Based upon the results of the risk assessment, evaluate the physical operation of the facility, and intervention points where human access could occur. Consider using one or a combination of the following:

Consider developing and implementing a **pre- opening/start-up and closing security checklist** in which key employees are assigned to check critical security areas for signs of tampering, burglary, vandalism or suspicious activities. Such checks may include visual inspections of the perimeter of buildings and secured areas (such as dump pits; control rooms; inventory storage areas, doors and windows; equipment; power sources and electrical boxes; and openings to exterior- located fans, particularly if they are located in insecure areas or where lighting is insufficient). Note and rectify any discrepancies.

Consider installing **locked gates on exterior ladders** to protect from unauthorized use and to prevent access to the top of storage tanks.

**Secure doors to shop and tool storage areas.**

**Restrict access to the facility's control room**, as well as computer process-control and data systems. **Safeguard information (e.g., computer systems)** with up-to-date anti-virus protection on computer server and individual operating units. Store back-

#### 5.6.4 Mengamankan Operasi Perusahaan :

Berdasarkan hasil penilaian risiko, evaluasi operasi fisik fasilitas, dan titik intervensi di mana akses manusia dapat terjadi. Pertimbangkan untuk menggunakan satu atau kombinasi dari yang berikut:


Pertimbangkan untuk mengembangkan dan mengimplementasikan daftar periksa/cheklist keamanan pra-buka / start-up dan penutupan di mana karyawan ditugaskan untuk memeriksa area keamanan kritis untuk tanda-tanda gangguan, pencurian, kerusakan atau kegiatan mencurigakan. Pemeriksaan tersebut dapat mencakup inspeksi visual perimeter bangunan dan area aman (seperti tempat pembuangan; ruang kontrol; area penyimpanan inventaris, pintu dan jendela; peralatan; sumber daya dan kotak listrik; dan bukaan yang berlokasi di luar) , terutama jika mereka berada di area yang tidak aman atau di mana pencahayaan tidak cukup). Catat dan perbaiki setiap perbedaan.

Pertimbangkan untuk memasang gerbang yang terkunci pada tangga tangga diluar/eksterior untuk melindungi dari penggunaan yang tidak sah dan untuk mencegah akses masuk keatas Gedung/fasilitas.

Amankan pintu untuk bengkel dan area penyimpanan alat.

Batasi akses ke ruang kontrol fasilitas, serta kontrol proses komputer dan sistem data.

Perlindungan terhadap Sistem informasi (mis., Komputer) dengan perlindungan anti-virus terkini di server komputer dan unit operasi individual. Simpan

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 14 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

up data offsite.

Secure access to power sources, such as power rooms and electrical panels, to prevent unauthorized entry and power disruption or sabotage.

Maintain current and accurate inventory records

#### 5.6.5 Restrict Access to Sensitive Information:

Be cautious about requests for information received by telephone or email. Do not provide information if the request appears suspicious or is from an unfamiliar person or organization.

Ask for such requests to be submitted in writing. Obtain as much information as possible from requestors with whom you are unfamiliar, including name, address, telephone number, references and reason for the request. Any reluctance by the requestor to provide such information should serve as a warning flag – don't cooperate further.

If there is any doubt about the appropriateness of releasing information – particularly information that might compromise security – refuse to provide it.

Companies web sites should be cautious not to post sensitive, security-related information about the company, its operations, or facility layout or /product lines. Do not display sensitive (such as facility diagrams) or private company information on company web site.

Be discreet about sharing any information contained in the facility security plan or accompanying documents.

cadangan data di luar kantor.

Pengamanan akses ke sumber daya listrik, seperti kamar listrik dan panel listrik, untuk mencegah masuknya yang tidak resmi dan gangguan daya atau sabotase.

Menyimpan catatan inventaris terkini dan akurat

#### 5.6.5 Batasi Akses ke Informasi Sensitif:

Berhati-hatilah dengan permintaan informasi yang diterima melalui telepon atau email. Jangan memberikan informasi jika permintaan tampak mencurigakan atau berasal dari orang atau organisasi yang tidak dikenal.


Permintaan seperti itu harus diajukan secara tertulis. Dapatkan informasi sebanyak mungkin dari pemohon yang tidak Anda kenal, termasuk nama, alamat, nomor telepon, referensi, dan alasan permintaan tersebut. Keengganan oleh pemohon untuk memberikan informasi tersebut harus berfungsi sebagai tanda peringatan - jangan bekerja sama lebih jauh.

Jika ada keraguan tentang kesesuaian pemberian informasi - khususnya informasi yang dapat membahayakan keamanan - jangan berikan.

Situs web perusahaan harus berhati-hati untuk tidak memposting informasi sensitif, terkait keamanan tentang perusahaan, operasinya, atau tata letak fasilitas atau lini produk. Jangan tampilkan sensitif (seperti diagram fasilitas) atau informasi perusahaan swasta di situs web perusahaan.

Hati hati dalam berbagi informasi apa pun yang terkandung dalam rencana keamanan fasilitas atau dokumen yang menyertainya.



	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 15 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

**Control access to all information** – including, but not limited to, documents, notes, photographs, diagrams and/or other work products – that contain sensitive, security-related information. Make sure such information is never left unattended by the originator or other authorized recipient. At the end of each workday, secure any such formation in a locked and controlled environment.

**Sensitive, security-related information** that is stored in electronic form should be maintained in a password-protected environment that is sufficiently secure from access by any unauthorized source.

No sensitive, security-related information should be transmitted through unsecure email.

Verbal communication of sensitive, security-related information should occur in environments where only those with a legitimate “need to know” may hear it.

**Kontrol akses ke semua informasi** - termasuk, tetapi tidak terbatas pada, dokumen, catatan, foto, diagram, dan / atau produk kerja lainnya - yang berisi informasi sensitif dan terkait keamanan. Pastikan informasi tersebut tidak pernah ditinggalkan tanpa pengawasan oleh pihak perusahaan atau penerima resmi lainnya. Pada akhir setiap hari kerja, amankan informasi tersebut di lingkungan yang terkunci dan terkendali.

**Informasi sensitif dan terkait keamanan** yang disimpan dalam bentuk elektronik harus dijaga dalam lingkungan yang dilindungi kata sandi yang cukup aman dari akses oleh sumber yang tidak sah.

Tidak ada informasi sensitif dan terkait keamanan yang boleh dikirimkan melalui email yang tidak aman.

Komunikasi verbal informasi sensitif dan terkait keamanan harus terjadi di lingkungan di mana hanya mereka yang "perlu tahu" yang boleh mendengarnya

5.6.6 Assess the feasibility of implementing the following steps to enhance the security of the facility's operating and personnel procedures:

Employee-Hiring Practices: When hiring:

Request resumes from applicants specifying their qualifications and references. Be cautious of applicants who offer incomplete information on employment applications.

Verify that all employees and applicants have appropriate legal SKCK(Surat Keterangan Catatan Kepolisian)-Police Security Clearance Letter

Depending upon the nature and


5.6.6. Menilai kelayakan menerapkan langkah-langkah berikut untuk meningkatkan keamanan operasi dan prosedur personel fasilitas:

Praktek Perekrutan Karyawan: Saat merekrut:

Meminta resume dari pelamar yang menentukan kualifikasi dan referensi mereka. Berhati-hatilah terhadap pelamar yang menawarkan informasi tidak lengkap tentang lamaran kerja.

Verifikasi bahwa semua karyawan dan pelamar memiliki Surat Keterangan Catatan Kepolisian (SKCK) yang sah - Surat Izin Keamanan Polisi

Bergantung pada sifat dan sensitivitas

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 16 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

sensitivity of the applicant's job function, check with multiple references for background checks to establish a prospective employee's qualifications. Consider using commercial services to conduct pre-placement background security checks for a certain level of employee, which involve checks of police. Make sure the third-party service is reputable and uses procedures designed to protect against unlawful discrimination.

For employees granted access to secure areas, maintain higher requirements for references, length of employment and other safeguards.

Be wary of transient or seasonal employees. Do not issue keys or access codes to employees who are seasonal or expected to be short-term.

**5.6.7 Employee Training (Security Awareness):** The most important threat- reduction measure is vigilance on the part of employees, their awareness of anything out-of-the-ordinary, and their prompt communication of that information to facility management or law enforcement personnel.

Instill security awareness in all employees so that security becomes part of their job when communicating and interacting with visitors, customers, vendors, truck drivers and fellow employees.

Conduct regular training to discuss the facility's security policies and procedures, the areas of potential risk, and the location of emergency exit routes and service shut-off points for utilities, fuel, hauling, fuel tank pumps, etc.

fungsi pekerjaan pelamar, tanyakan beberapa referensi untuk pemeriksaan latar belakang untuk menetapkan kualifikasi calon karyawan. Pertimbangkan untuk menggunakan layanan komersial untuk melakukan pemeriksaan keamanan latar belakang pra-penempatan untuk tingkat karyawan tertentu, yang melibatkan pemeriksaan polisi. Pastikan layanan pihak ketiga memiliki reputasi dan menggunakan prosedur yang dirancang untuk melindungi terhadap diskriminasi yang melanggar hukum.

Untuk karyawan yang diberikan akses ke area yang khusus, pertahankan persyaratan yang lebih tinggi untuk referensi, lama kerja dan perlindungan lainnya.


Berhati-hatilah terhadap karyawan sementara atau musiman. Jangan menerbitkan kunci atau kode akses untuk karyawan yang musiman atau diperkirakan akan menjadi jangka pendek

**5.6.7. Pelatihan Pegawai (Kesadaran Keamanan):** Tindakan pengurangan ancaman yang paling penting adalah kewaspadaan pada karyawan, kesadaran mereka akan sesuatu yang tidak biasa, dan komunikasi cepat mereka atas informasi itu kepada manajemen fasilitas atau penegakan hukum personil.

Menanamkan kesadaran keamanan di semua karyawan sehingga keamanan menjadi bagian dari pekerjaan mereka ketika berkomunikasi dan berinteraksi dengan pengunjung, pelanggan, vendor, pengemudi truk dan sesama karyawan.

Lakukan pelatihan rutin untuk membahas kebijakan dan prosedur keamanan fasilitas, bidang-bidang risiko potensial, dan lokasi rute keluar darurat



	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 17 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

Conduct refresher training periodically (*annually, etc.*) for existing employees; when hiring new employees; and whenever substantive changes to security policies or procedures are made.

**5.6.8 Resignation/Termination of Employees: Upon resignation or termination of the employee:**

Collect the departing employee's identification cards, photos or other items that demonstrate employment with the company.

Collect all keys to vehicles, secured buildings and other secured areas that may have been issued to the departing employee.

Collect cell phones, two-way radios and other company electronic devices that may have been issued to the employee.

Suspend access to information/computer systems to prevent former employees from gaining access to sensitive information. This may involve changing passwords or other access codes for the facility's computer system.

Inform customers when there is a change in the name of the employee servicing those accounts to prevent unauthorized access to the customer's property.

Update company records, telephone lists, web sites and other materials that list employee names or authorize access to company facilities, shipments, records or other information.

dan titik-titik penghentian layanan untuk utilitas, bahan bakar, jalur hauling, pompa tangki bahan bakar, dll.

Melakukan pelatihan penyegaran secara berkala (tahunan, dll.) Untuk karyawan yang ada; saat merekrut karyawan baru; dan kapan pun perubahan substantif terhadap kebijakan atau prosedur keamanan dilakukan.

**5.6.8. Pengunduran diri / Pemutusan Hubungan Kerja Karyawan: Setelah pengunduran diri atau pemutusan hubungan kerja dari karyawan:**

Mengumpulkan kartu identitas karyawan, foto, atau item lain yang menunjukkan pekerjaan dengan perusahaan.


Kumpulkan semua kunci kendaraan, gedung yang diamankan dan area aman lainnya yang mungkin telah dikeluarkan untuk karyawan yang berangkat.

Kumpulkan ponsel, radio dua arah, dan perangkat elektronik perusahaan lain yang mungkin telah dikeluarkan untuk karyawan.

Tangguhkan akses ke sistem informasi / komputer untuk mencegah bekas karyawan mendapatkan akses ke informasi sensitif. Ini mungkin melibatkan mengubah kata sandi atau kode akses lain untuk sistem komputer fasilitas.

Menginformasikan pelanggan ketika ada perubahan dalam nama karyawan yang melayani akun tersebut untuk mencegah akses tidak sah ke properti pelanggan.

Perbarui catatan perusahaan, daftar telepon, situs web, dan materi lain yang mencantumkan nama karyawan atau

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 18 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

**5.6.9 Outside Contractor/Vendor Policies: When using outside contractors and vendors, consider the following procedures:**

Check background, references and insurance coverage for outside contractors or other outside groups before granting access to the facility. In the contract with such parties, outline the parameters and conditions that apply to those assigned to the site.

Inform outside contractors about established company safety and security procedures. Conduct annual training/orientation for regular contractors to reinforce the facility's safety and security policies.

Consider whether to use a pre-work checklist with individual contractors to ensure they understand the facility's safety rules (*e.g., hot work permits, lock-out/tag-out procedures, etc.*); areas of the plant where they are allowed access; and the need to actively manage their own personnel and the security of all materials and tools used at the worksite.

Inform outside contractors about areas of the facility to which they are allowed access.

Require outside contractors to sign in and be issued company credentials so they can be identified easily prior to being granted access to the facility.

Consider requiring an employee escort for contractors using hazardous or dangerous materials on site (such as chemicals or items that could be used as a weapon).

**5.6.9. Kebijakan Kontraktor / Vendor Luar: Ketika menggunakan kontraktor dan vendor luar, pertimbangkan prosedur berikut:**

mengizinkan akses ke fasilitas perusahaan, pengiriman, catatan, atau informasi lainnya.

Periksa latar belakang, referensi dan cakupan asuransi untuk kontraktor luar atau kelompok luar lainnya sebelum memberikan akses ke fasilitas. Dalam kontrak dengan pihak-pihak tersebut, uraikan parameter dan ketentuan yang berlaku untuk yang ditugaskan ke lokasi.


Briefing kontraktor tentang prosedur keselamatan dan keamanan perusahaan yang berlaku. Lakukan pelatihan / orientasi tahunan untuk kontraktor reguler untuk memperkuat kebijakan keselamatan dan keamanan fasilitas.

Pertimbangkan untuk menggunakan daftar periksa/checklist pra-kerja dengan masing-masing kontraktor untuk memastikan mereka memahami aturan keselamatan fasilitas (mis., Izin kerja panas, prosedur penguncian / penandaan, dll.); area kerja di mana mereka diizinkan mengakses; dan kebutuhan untuk secara aktif mengelola personel mereka sendiri dan keamanan semua bahan dan alat yang digunakan di tempat kerja.

Briefing/sosilaisaikan kontraktor tentang area fasilitas yang mereka boleh dimasuki.

Mewajibkan kontraktor untuk masuk dan diberikan kartu pengenalan perusahaan sehingga mereka dapat diidentifikasi dengan mudah sebelum diberikan akses ke fasilitas.

Pertimbangkan untuk meminta

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 19 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

pengawasan karyawan untuk kontraktor yang menggunakan bahan berbahaya atau berbahaya di lokasi (seperti bahan kimia atau barang yang dapat digunakan sebagai senjata)

#### 5.6.10 Identification (ID) Card

A standardized ID card shall be worn by Employees whilst at the Office. The ID card shall consist only of a photograph and name of the employee. The photograph on the ID card shall be a frontal view capturing the head of the individual, it shall be an accurate depiction of the individual and there must not be any items in the photograph that obscure or partially obscure the individual's face or head. ID cards shall be worn in clear view, above the waist, at all times whilst at the Office/site.

The HRD is responsible for issuing the ID card. A record of the issuance of the ID card shall be kept on an ID card register (logistic support staff)

#### 5.6.10. Kartu Identifikasi (ID)

Kartu ID standar harus dikenakan oleh Karyawan saat berada di Kantor. Kartu ID hanya terdiri dari foto dan nama karyawan. Foto pada kartu ID harus berupa tampilan depan yang menangkap wajah dengan jelas, itu harus merupakan gambaran yang akurat dari individu tersebut dan tidak boleh ada barang dalam foto yang mengaburkan atau mengaburkan sebagian wajah atau kepala individu. Kartu ID harus dikenakan dalam tempat yang jelas, di atas pinggang, setiap saat saat berada dilingkungan kerja.

HRD bertanggung jawab untuk mengeluarkan kartu ID. Catatan penerbitan kartu ID harus disimpan pada register kartu ID (staf pendukung logistik)

#### 5.6.11 Electronic Access Control System (EACS)


Access and egress to the plant/working area and buildings is controlled by a building Electronic Access Control System (EACS). The system comprises of EACS Readers located for entry purposes that are activated by an EACS Card. All employees, visitor, vendor and clients will be issued with an EACS Card at the lobby to access office and/or floors at the Buildings for which they have been authorized to enter. EACS Card at an exit card scanner is also required at the main entrance/gates/lobby.

Employee will be provided by PT INDEXIM COALINDO Access to the main office entrance require an EACS

#### 5.6.11. Sistem Kontrol Akses Elektronik (EACS)

Akses dan jalan keluar ke lokasi kerja dan bangunan dikendalikan oleh gedung Electronic Access Control System (EACS). Sistem ini terdiri dari Pembaca EACS yang terletak untuk tujuan entri yang diaktifkan oleh Kartu EACS. Semua karyawan, pengunjung, vendor, dan klien akan diberikan Kartu EACS di lobi untuk mengakses kantor dan / atau lantai di Gedung tempat mereka diizinkan untuk masuk. Kartu EACS di pemindai kartu keluar juga diperlukan di pintu masuk / gerbang / lobi utama.

Karyawan akan diberikan oleh PT INDEXIM COALINDO Akses ke pintu masuk kantor utama membutuhkan

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 20 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

Card between the hours of 0800 to 1700hrs, Monday to Friday. An EACS Card will be required for access at all other times upon notification to Security on duty and required their supervisor approval.

Kartu EACS antara pukul 08.00 hingga 17.00, Senin hingga Jumat. Kartu EACS akan diperlukan untuk akses setiap saat setelah pemberitahuan ke Keamanan yang bertugas dan memerlukan persetujuan penyelia mereka

#### 5.6.12 Security Personnel

PT INDEXIM COALINDO provides security guard for the premises to provide 24 hour security presence at the main entrance, gates and others restricted area includes patrol and response team.

Security guards supplied by the Contractor provide 24 hour security presence at the site. Twelve (12) clocking rounds are conducted by the Premises security guards daily. Contractor Supervisor conducts a routine weekly inspection to monitor the performance and situation of the premises.

The Site Security shift system and manning is detailed as follows:

##### Morning Shift

Hours of Duty are 0700 until 19:00. Morning shift for security administrative duties, access control and roofing patrol during period of times.

##### Night Shift

Hours of duty are from 19:00 until 07:00 daily. The guard stationed and conduct a routine patrol at hourly basis.

Guard's duty posts shall be changed at the discretion of the Contractor Shift Supervisor dependent upon the need to increase guard presence at locations of specific projects being conducted within the facility.

#### 5.6.12. Personel Keamanan

PT INDEXIM COALINDO menyediakan penjaga keamanan di lokasi untuk menyediakan kehadiran keamanan 24 jam di pintu masuk utama, gerbang dan area terlarang lainnya termasuk patroli dan tim respons.

Petugas keamanan, yang disediakan oleh Kontraktor menyediakan kehadiran keamanan 24 jam di lokasi. Pola 12 jam putaran waktu dilakukan oleh satuan keamanan setiap hari. Pengawas Kontraktor melakukan inspeksi mingguan rutin untuk memantau kinerja dan situasi tempat.

Sistem dan manning shift Keamanan Situs dirinci sebagai berikut:

##### Pergeseran Pagi


Jam tugas adalah 0700 hingga 15:00. Shift pagi untuk tugas-tugas administrasi keamanan, kontrol akses dan patroli atap selama periode waktu.

##### Pergeseran Malam

Jam tugas mulai dari 19:00 hingga 07:00 setiap hari. Penjaga itu ditempatkan dan melakukan patroli rutin setiap jam.

Ketentuan Pos jaga sekuriti harus diubah atas kebijakan Pengawas Kontraktor tergantung pada kebutuhan untuk meningkatkan kehadiran penjaga di lokasi proyek/kerja tertentu yang dilakukan dalam fasilitas.

Patroli keamanan dirancang sedemikian

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 21 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

Security patrol within the facility and all area will be implemented to allow for maximum guard presence in all access and exit gates, static post locations and routine (hauling) patrolling of the Area of Responsibility.

Flood lights installed around the perimeters and provide main external lighting to the Premises.

Vehicular access and egress to and from the Premises is controlled by the guard with manual gate system. This system logs vehicles entry and exit details daily.

#### 5.6.13 COMPANY SECURITY PERSONNEL AND RESOURCES

The PT INDEXIM COALINDO will appointed the Security Coordinator/Manager. The role is to ensure that:

- Security measures are based on sound assessments of risk, are appropriate to offset the risks, and are cost effective.
- On an ongoing basis, employees are made aware of security risks and of their personal responsibilities to maintain security.
- The need for security assessment, plans and measures will be considered at the earliest stage of new projects, such as renovation or construction of Company facilities.
- Security resources are allocated, that security responsibilities are being met, and that senior management is assured of the adequacy of the security program.

rupa untuk memaksimalkan keberadaan satuan pengamanan terutama di jalur hauling dan area tanpa pos jaga.


Lampu dipasang di sekeliling perimeter dan memberikan pencahayaan eksternal disekitar bangunan.

Akses dan jalan keluar kendaraan ke dan dari lokasi dikontrol oleh penjaga dengan sistem gerbang manual. Sistem ini mencatat rincian masuk dan keluar kendaraan setiap hari.

#### 5.6.13. PERSONEL DAN SUMBERDAYA KEAMANAN PERUSAHAAN

PT INDEXIM COALINDO akan menunjuk Koordinator / Manajer Keamanan. Peran tersebut adalah untuk memastikan bahwa:

- Langkah-langkah keamanan didasarkan pada penilaian risiko yang tepat, sesuai untuk mengimbangi risiko, dan hemat biaya.
- Secara berkelanjutan, karyawan disadarkan akan risiko keamanan dan tanggung jawab pribadi mereka untuk menjaga keamanan.
- Perlunya penilaian keamanan, rencana dan langkah-langkah akan dipertimbangkan pada tahap paling awal dari proyek baru, seperti renovasi atau pembangunan fasilitas Perusahaan.
- Sumber daya keamanan dialokasikan, bahwa tanggung jawab keamanan sedang dipenuhi, dan bahwa manajemen senior dijamin akan kecukupan program keamanan.
- Kontak dibuat dengan pejabat penegak hukum setempat,

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 22 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

- Contacts are established with local law enforcement officials, emergency responders, security personnel or other public safety agencies with jurisdiction.

emergency/ darurat, personil keamanan atau lembaga keselamatan publik lainnya dengan yurisdiksi.

#### 5.6.14 CCTV System

To provide the CCTV System that could detect intruders, alert the security guards and provide a permanent record of activity from all cameras.

Numbers of CCTV's operational 24/7 is located around the perimeter, gate entry/out, hauling road intersections (critical one/high risk area) and critical area within the Premises provided and monitored by SCC (Security Command Center) located at Main Gate. Recordings are kept for an average of 30 days on a hard disk.

Stand alone CCTV on each post shall be maintained for 24 hours operational and all data shall be downloaded on regular schedule.

Supplementary objectives of the design:

- To provide general surveillance of the facility without compromising overall security includes : emergency exit doors, restricted area, all main access doors, plant, receiving area, control room and Data center.
- To provide a deterrent to crime and vandalism in COMPANY premises
- To enable 24 hours monitoring of the designated and critical areas
- To enable clear identification of miscreants within the range of cameras
- To provide continuous recording off all cameras in the system
- To enable e rapid movement of any camera to pre-set positions of pan-

#### 5.6.14. Sistem CCTV

Menyediakan Sistem CCTV yang dapat mendeteksi penyusup, dan mengaktifkan response penjaga keamanan dan merekam semua aktifitas dari seluruh kamera.


Jumlah operasional CCTV 24/7 terletak di area pintu masuk/keluar, persimpangan jalan hauling/rawan. Kantor manajemen, dan area kritikal lainnya. Dipantau oleh SCC (Pusat Komando Keamanan) yang berlokasi di Gerbang Utama. Rekaman disimpan selama rata-rata 30 hari pada hard disk.

CCTV yang berdiri sendiri pada setiap pos harus dipelihara selama 24 jam operasional dan semua data harus diunduh sesuai jadwal reguler.

Tujuan tambahan dari desain:

- Untuk memberikan pengawasan umum terhadap fasilitas tanpa mengorbankan keseluruhan keamanan meliputi: pintu keluar darurat, area terbatas, semua pintu akses utama, instalasi, area penerima, ruang kontrol dan pusat data.
- Untuk memberikan pencegah kejahatan dan vandalisme di tempat kerja.
- Untuk mengaktifkan pemantauan 24 jam pada area yang ditunjuk dan kritis
- Untuk memungkinkan identifikasi yang jelas dari pelanggar dalam jangkauan kamera



	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 23 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

- tilt and zoom
- To provide independent viewing of any camera at the Control room
- To enable live, real time recording of selected cameras through the LAN or other system

- Untuk memberikan perekaman yang berkelanjutan dari semua kamera dalam sistem
- Mempunyai kemampuan untuk PTZ
- Untuk memberikan tampilan independen dari kamera apa pun di ruang Kontrol
- Untuk mengaktifkan perekaman langsung, real-time dari kamera yang dipilih melalui LAN atau system lainnya

## 5.7 Security Program & Planning

## 5.7 Program Keamanan dan Perencanaan

5.7.1 Every business process unit should determine each working program and plan according to established functional plan and its practices to fulfill the goals and purposes of each performance key indicator.

5.7.1 Setiap bisnis proses harus menentukan perencanaan dan program kerja sesuai dengan perencanaan fungsi yang telah ditentukan serta upayanya memenuhi tujuan dan sasaran pada masing-masing indikator pencapaian kinerjanya.

5.7.2 In order to identify potential area and the practice to decrease corruption, collusion, and nepotism according to existing values within PT INDEXIM COALINDO Code of Conduct, it shall be done in Compliance & Governance Department working plan.

5.7.2 Dalam upaya mengidentifikasi area yang memiliki potensi dan upayanya mengurangi terjadinya Korupsi, Kolusi dan Nepotisme sesuai dengan nilai – nilai yang ditentukan dalam PT INDEXIM COALINDO Code of Conduct maka dilakukan dalam program kerja Departemen Compliance & Governance.

## 5.8 Guard Personnel Competence, Care, and Training


## 5.8 Pelatihan tenaga security, Kepedulian dan Kompetensi Personel

5.8.1 In accordance to functions within Integrated PT INDEXIM COALINDO security approach system. Training Master Plan (TMP) is a method used to define exact training needs. By comparing required knowledge and skill level in handling a working task with own knowledge and skill.

5.8.1 Sesuai dengan fungsi pada PT INDEXIM COALINDO yang terintegritas. Rencana Induk Pelatihan (TMP) adalah suatu metode untuk menentukan kebutuhan pelatihan yang senyatanya.

- Goal setting
- Training Need Analysis
- Development
- Realization
- Evaluation and result measurement

Dengan cara membandingkan antara tingkat pengetahuan dan ketrampilan yang diperlukan untuk melaksanakan tugasnya dengan tingkat pengetahuan dan ketrampilan yang dimiliki. terdiri dari:

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 24 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

- Penetapan sasaran
- Analisa kebutuhan pelatihan
- Pengembangan
- Realisasi
- Pengukuran dan evaluasi hasil

5.8.2 Every function in related Business Process Department is to develop their training needs and approved by related Department Manager, through:

- Training goal setting
- Training method defining which
- Determining training attendees
- Choosing the instructures and prepare for the training materials
- Designing initial test material, post-test, and implementation test in each work unit
- Preparing required infrastructure
- Setting up training schedule
- Training costs budgeting

5.8.2 Fungsi setiap Bisnis Proses Departemen terkait adalah mengembangkan rencana pelatihan berdasarkan identifikasi kebutuhan pelatihan yang telah disetujui oleh Manajer Departemen terkait, dengan:

- Menetapkan tujuan pelatihan
- Menetapkan metode pelatihan yang
- Menentukan peserta pelatihan
- Memilih instruktur dan mempersiapkan bahan pelatihan
- Merancang bahan tes awal, tes akhir dan tes penerapan di unit kerja
- Mempersiapkan infrastruktur
- Membuat jadwal pelatihan
- Menganggarkan biaya pelatihan

5.8.3 Related to third party involvement, it is contractually stated that personnel training needs should be provided by PT INDEXIM COALINDO, therefore it is required to deliver Training Needs Analysis to PT INDEXIM COALINDO management

5.8.3 Terkait dengan aktifitas pihak ketiga yang secara kontraktual dinyatakan bahwa pemenuhan kebutuhan pelatihan personel harus dipenuhi oleh pihak PT INDEXIM COALINDO maka diperlukan penyampaian Analisa Kebutuhan Pelatihan yang disampaikan kepada PT INDEXIM COALINDO management.

5.8.4 Details on Personnel Training, Care, and Competence shall refer to the Training & Competence Development.

5.8.4 Detail mengenai Pelatihan, kepedulian dan kompetensi personel mengacu pada Training & Competence Development


## 5.9 Consultancy, Communications, and Participation

## 5.9 Konsultasi, Komunikasi & Partisipasi

5.9.1 The role of consultancy and participation which involve Company's Management and the community surrounding is forming active security partnership for the community through a

5.9.1 Peran konsultasi dan partisipasi yang melibatkan perwakilan perusahaan dan komunitas sekitar pabrik sebagai upaya secara aktif membentuk kemitraan pengamanan masyarakat melalui Forum Konsultasi Masyarakat dilakukan secara periodik untuk membangun pemahaman, kepercayaan dan saling menghormati antara perusahaan dan



	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 25 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

periodic Community Advisory Panel to build understanding, trust, and respect among both sides.

5.9.2 Both internal and external communications channels are well established as an effort to socialize corporate programs to all relevant stakeholders through:

- PT INDEXIM COALINDO Portal
- Business Briefing
- Media publication
- Media analysis
- Press conference

#### 5.10 Document and Data Control

To ensure that every requirements on Security Management System is fulfilled, PT INDEXIM COALINDO follows the procedure of Record, Document & Data Control where it describes in details about creation process, changes, approvals, numbering, arrangement/formatting, distribution, and management system document drawing.

#### 5.11 Emergency Handling

5.11.1 In providing guidelines to identify an emergency situation and develop prevention plan, response, and reduce emergency situation for human protection and minimize pollution and other loss potentials, PT INDEXIM COALINDO Emergency Preparedness & Response. Then, every site will have to make site-specific report and its emergency response plan by referring to this procedure.

masyarakat.

5.9.2 Saluran komunikasi yang telah ditentukan baik secara internal maupun eksternal sebagai upaya sosialisasi terhadap program – program perusahaan kepada seluruh stakeholder yang terkait dapat dilakukan dengan hal berikut yang tidak terbatas pada:


- PT INDEXIM COALINDO Portal
- Business Briefing
- Pemberitaan Media
- Analisa Media
- Konferensi Press

#### 5.10 Pengendalian Dokumen dan Catatan

Untuk memastikan terpenuhinya persyaratan terhadap ketentuan sistem manajemen Pengamanan, PT INDEXIM COALINDO mengacu pada prosedur Record, Document & Data Control dimana secara detail menjelaskan tentang proses pembuatan, perubahan, persetujuan, penomoran, pengaturan/formating, distribusi dan penarikan dokumen system manajemen.

#### 5.11 Penanganan Keadaan Darurat

5.11.1 Dalam menyediakan panduan terhadap kebutuhan untuk mengidentifikasi situasi darurat yang dapat diperkirakan sebelumnya dan dalam mengembangkan perencanaan untuk mencegah, menanggapi dan meringankan situasi darurat untuk tujuan perlindungan manusia dan meminimalkan polusi serta kerugian lainnya PT INDEXIM COALINDO mengacu pada Emergency Preparedness & Response. Setiap site selanjutnya harus membuat pertanggung jawaban site-spesific dan rencana tanggap keadaan darurat dengan merujuk pada prosedur ini.

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 26 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

5.11.2 To determine an emergency response plan with wider scope where crisis condition may impact to business process continuity and Crisis Management Team function is active, it is arranged more detail in PT INDEXIM COALINDO & Emergency Management Business Continuity Management – System Description & Plan

## **5.12 IT Operation Control**

### **5.12.1 IT Operation**

To ensure that all policies and their implementation on PT INDEXIM COALINDO IT Operation which is valid to all IT Operation Activities done by PT INDEXIM COALINDO employees who use IT hardwares and softwares to support their working performance.

## **5.13 Physical Security Management**

- Security Management on company's physical facilities is determined through an established security monitoring parameter on sites which consider corporate operational factors in each sites's posting document order.
- In case where operational implementation is done by SECURITY SERVICES PROVIDER then The Operation Planning and Management should follow PT INDEXIM COALINDO's direction and mention in the report that operational work is done by valid procedure, supported with registered operation forms

5.11.2 Untuk menentukan persyaratan perencanaan tanggap darurat dengan cakupan yang lebih luas dimana dapat menimbulkan kondisi krisis yang mungkin berdampak pada gangguan kelangsungan bisnis proses dan mengaktifkan fungsi Team Manajemen Krisis diatur lebih detail pada PT INDEXIM COALINDO Crisis & Emergency Management Business Continuity Management – System Description & Plan


## **5.12 Pengendalian Operasi IT**

### **5.12.1 Informasi & Teknologi Operasional**

Untuk memastikan bahwa kebijakan dan pelaksanaan strategi terhadap operasional IT terlaksana dengan baik dan benar sebagaimana pula pemenuhan persyaratan PT INDEXIM COALINDO IT Operation yang berlaku pada seluruh aktifitas operational IT baik di dalam maupun diluar tempat kerja bagi karyawan PT INDEXIM COALINDO yang menggunakan perangkat IT untuk mendukung aktifitas kinerjanya.

## **5.13 Pengendalian Pengamanan Fisik**

- Pengendalian pengamanan terhadap fasilitas fisik perusahaan ditentukan melalui penetapan perimeter pemantauan keamanan pada lokasi-lokasi yang telah ditetapkan dengan mempertimbangkan faktor – faktor operasional perusahaan yang diatur selanjutnya dalam dokumen pos order pada setiap lokasi pabrik.
- Dalam hal pelaksanaan pengendalian operasional yang dilakukan oleh BUJP maka Perencanaan dan Pengendalian Operasional harus berdasarkan ketentuan dari PT INDEXIM COALINDO yang kemudian dijabarkan pada pernyataan kerja pihak ketiga

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 27 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

- Equipment maintenance review held by third party should be done periodically and current equipment status is filed to ensure the equipment properness.

#### 5.14 Financial Control

A review process is done to ensure that all financial related activities in business process are running well as required through a periodic evaluation held by Internal Control.

#### 5.15 Provider Operation Control

- There is a Service Level Agreement for operation control, used as service agreement by Indexim Coalindo which will be monitored and controlled.
- In all core business processes, there are procedures to ensure that current processes are working on track

#### 5.16 Data, Analysis and Working Performance Report

- 5.16.1 Every disturbance investigation report and threats or identified situation related to problem cause that is potential in risking the business process continuity, should be reported according to current reporting procedure. Furthermore, the procedure shall detect, analyze, and eliminate all inappropriate potentials.

dengan menjalankan prosedur Operasional yang sesuai dan diperlukan serta laporan dari formulir Operasional didokumentasikan.

- Pemantauan terhadap peralatan yang digunakan oleh pihak ketiga harus dilakukan secara berkala dan status peralatan terakhir didokumentasikan untuk memastikan kehandalan peralatan

#### 5.14 Finansial Kontrol


Proses tinjauan untuk memastikan bahwa seluruh aktifitas yang terkait dengan perihal keuangan pada setiap bisnis proses berjalan sesuai dengan persyaratan yang telah ditentukan maka dilakukan evaluasi melalui internal kontrol secara periodik

#### 5.15 Operational Kontrol BUJP

- Untuk pengendalian operasional terdapat dokumen persetujuan tingkat pelayanan Service Level Agreement, yang digunakan sebagai perjanjian pelayanan yang harus dilakukan secara online.
- Pada setiap bisnis proses utama terdapat prosedur untuk memastikan bahwa tahapan proses berjalan sesuai dengan ketentuan

#### 5.16 Pelaporan Data, Analisa dan Evaluasi Kinerja

- 5.16.1 Setiap hasil investigasi gangguan dan ancaman atau situasi yang teridentifikasi dan berhubungan dengan akar masalah yang memiliki potensi dapat mengganggu keamanan kelanjutan bisnis proses harus dilaporkan sesuai dengan prosedur pelaporan yang ada. Selanjutnya

	PT INDEXIM COALINDO	Date: 1 September 2019	
		Version: 1.0	Page: 28 / 28
	Corporate Security Guideline	DOC.NO. xxxxxx	
Title: Security Management System			

5.16.2 Performance evaluation on Purpose and Goals established in business process related to Security Management System within PT INDEXIM COALINDO is done periodically through a general audit process by internal and external parties and management review

prosedur dapat mendeteksi, menganalisa dan menghilangkan penyebab potensial dari ketidaksesuaian.

5.16.2 Evaluasi kinerja terhadap Tujuan dan Sasaran yang ditetapkan pada bisnis proses yang terkait terhadap pengembangan dan pelaksanaan Sistem Manajemen Pengamanan di PT INDEXIM COALINDO dilakukan secara periodik melalui proses audit secara keseluruhan yang dilakukan internal maupun eksternal dan tinjauan manajemen

5.16.3 Top Management of PT INDEXIM COALINDO and BUJP should make a periodic management review on implemented Security Management System to measure the implementation and achievement based on security policy and purpose. During this review the continual improvement's opportunities on performance of security management is also concerned.

5.16.3 Pimpinan department PT INDEXIM COALINDO dan BUJP harus mengkaji penerapan Sistem Manajemen Pengamanan secara periodik untuk menilai penerapan dan kesesuaian pencapaian berdasarkan kebijakan keamanan dan tujuan keamanan. Dalam tinjauan ini peluang peningkatan berkelanjutan atas kinerja sistim pengamanan juga dibahas.