PT INDEXIM COALINDO

SECURITY RISK ASSESMENT

PENILAIAN RESIKO KEAMANAN

DOC NO. XXXXX

CONFIDENTIAL

TABLE OF CONTENTS

1 PURPOSE

This procedure describes the methodology for doing security risk assessment, determine the risk level and recommend control plan and its improvement.

1 TUJUAN

Prosedur ini menjelaskan mengenai metodologi untuk melakukan identifikasi dan evaluasi tingkat resiko pengamanan serta mengusulkan rencana pengendalian dan perbaikannyanya.

2 SCOPE

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

2 RUANG LINGKUP

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

3 REFERENCES

3.1 Indexim Coalindo Corporate Manual (HSEQ-Management System)

3.2 Indexim Coalindo Security Management System

3. REFERENSI

3.1 Indexim Coalindo Corporate Manual (HSEQ-Management System)

3.2 Security Management System

4 DEFINITION

4.1 Security threat identification is a process to find all threat potency to security aspects in some activity from working environment, equipment and workers.

4.2 Security Risk Assessment methodology is a process to identify risk level of some activities base on exposure, probability and consequence.

4.3 Assets : Any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property. For purposes of this guideline, people are included as assets.

4. DEFINISI

4.1 Identifikasi ancaman keamanan adalah suatu proses untuk menemukan seluruh potensi ancaman terhadap aspek keamanan yang ada pada suatu aktivitas dari lingkungan kerja, peralatan dan pekerja itu sendiri.

4.2 Metode Penilaian Resiko Keamanan adalah suatu proses untuk mengidentifikasi tingkatan resiko/ ancaman dari beberapa aktivitas berdasarkan paparan, kemungkinan terjadi dan konsekuensinya

4.3 Aset : Sesuatu yang nyata atau milik pribadi yang bersifat nyata or tidak nyata, yang dimiliki oleh suatu perusahaan atau milik perorangan yang dapat diberikan atau dinyatakan dalam nilai monoter. Kekayaan intangible meliputi goodwill, kepemilikan informasi, dan kekayaan yang terkait. Dalam panduan ini manusia dimasukkan

sebagai asset

4.4 Cost/Benefit Analysis: A process in planning, related to the decision to commit funds or assets. This is a systematic attempt to measure or analyze the value of all the benefits that accrue from a particular expenditure. Usually, this process involves three steps:
- Identification of all direct and indirect consequences of the expenditure.
- Assignment of a monetary value to all costs and benefits resulting from the expenditure.
- Discounting expected future costs and revenues accruing from the expenditure to express those costs and revenues in current monetary values.

4.4 Analisa Untung/Rugi: Merupakan suatu proses dalam perencanaan yang berhubungan dengan keputusan pengadaan pendanaan atau asset. Hal ini merupakan cara sistematik untuk mengukur atau menganalisa nilai dari semua manfaat yang ditambahkan dari suatu pembelanjaan modal yang utama. Biasanya, proses ini melibatkan tiga tahapan :
- Identifikasi semua konsekuensi langsung dan tidak langsung dari pembelanjaan atau pengeluaran
- Pengenaan nilai moneter terhadap semua biaya dan manfaat yang dihasilakn dari pengeluaan.
- Diskon biaya biaya yang akan datang dan pendapatanyang diakrual dari pengeluaran untuk menggambarkan biaya biaya tersebut dan pendapatan di dalan nilai moneter saat ini.

4.5 Events : Something that happens; a noteworthy happening. In the security context, this usually represents an occurrence such as a security incident, alarm, medical emergency, or related episode or experience.

4.5 Kejadian : Suatu kejadian; atau kejadian penting. Dalam hubungannya dengan keamanan biasanya menggambarkan suatu peristiwa yang merupakan insiden keamananan, peringatan, emergensi secara medis, atau pengalaman yang terkait dengan keamanan .

4.6 Goodwill : The value of a business that has been built up through the reputation of the business concern and its owners.

4.6 Goodwill : Nilai dari suatu bisnis yang sudah dibangun melalui reputasi yang berhubungan dengan aspek bisnis dan pemiliknya.

4.7 Loss Event : An occurrence that actually produces a financial loss or negative impact on assets. Examples include security incidents, crimes, civil disturbance, natural hazards, or disasters.

4.7 Kejadian Kehilangan : Suatu kejadian yang mengakibatkan kehilangan secara financial atau dampak negatif pada aset. Sebagai contoh meliputi insiden keamanan, tindakan kriminal, demo dengan kekerasan, ancaman atau bahaya dari alam, atau bencana.

4.8 Natural Disaster : A naturally occurring calamitous event bringing great damage, loss, or destruction such as tornadoes, hurricanes, earthquakes, and related

4.8 Bencana Alam : Suatu peristiwa alam yang menyebabkan kerusakan hebat, kerugian atau penghancuran yang dakibatkan oleh misalnya ; tornado, badai, gempabumi dan

occurrences.

kejadian kejadian yang terkait.

4.9 Probability : The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes.

4.9 Kemungkinan Terjadi: Suatu kesempatan, atau dalam beberapa kasus, kepastian secara metematis yang mungkin terjadi; merupakan rasio jumlah kemungkinan yang dihasilkan dalam kejadian terhadap jumlah total semua kemungkinan yang ada.

4.10 Qualitative : Relating to that which is characteristic of something and which makes it what it is

4.10 Kualitatif : berhubungan dengan karateristik dari sesuatu dan yang membuat sesuatu itu sebagaimana adanya.

4.11 Quantitative : Relating to, concerning, or based on the amount or number of something, capable of being measured or expressed in numerical terms

4.11 Kuantitatif : berhubungan dengan, mengenai , atau didasarkan pada jumlah dari sesuatu, yang dapat diukur atau dinyatakan dalam bentuk numerik.

4.12 Risk : The possibility of loss resulting from a threat, security incident, or event.

4.12 Resiko : Kemungkinan kehilangan yang dihasilkan dari sesuatu ancaman, kejadian keamanan atau peritiwa.

4.13 Risk Analysis : A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.

4.13 Analisa Resiko : Merupakan pengujian yang lengkap terhadap penilaian resiko, evalusi resiko, dan alternatif manajemen resiko, yang dilaksanakan untuk memahami sifat yang tidak diinginkan, konsekuensi negative terhadap kehidupan manusia, kesehatan, harta, atau lingkungan; sebuah proses analisa untuk memberikan informasi tentang peristiwa peristiwa yang tidak diharapkan; sebuah proses kuantifikasi dari kemungkinan kemungkinan dan konsekuensi yg diharapkan untuk resiko yang teridentifikasi.

4.14 Risk Assessment: The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.

4.14 Penilaian Resiko: Sebuah proses untuk menilai resiko resiko internal maupun eksternal terhadap suatu entity, asset atau personil.

4.15 Security Incident: A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer,

4.15 Kejadian Keamanan: Suatu kejadian yang berhubungan dengan keamanan atau tindakan yang mungkin menyebabkan kematian, terluka atau kehilangan moneter.

or supplier on company property would be one example of a security incident.	Serangan terhadap karyawan, pelanggan atau pemasok kepada perusahaan adalah merupakan contoh insiden keamanan.
4.16 Security Vulnerability: An exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person.	4.16 Kerawanan Keamanan : suatu keadaan yang dapat dieksploitasi; kelemahan keamanan yang dapat dieksploitasi pada sesuatu fasilitas, badan, lokasi atau seseorang
4.17 Site : A spatial location that can be designated by longitude and latitude.	4.17 Site : Suatu lokasi yang berbentuk ruang yang dapat digambarkan garis bujur dan garis lintang yang merupakan batas batas area.
4.18 Multi discipline team is trained functional team which build permanently for identify threat and to do Risk Assessment and control measures.	4.18 Multi Disiplin Tim: adalah tim fungsional terlatih yg dibentuk permanen untuk melakukan identifikasi ancaman dan melakukan penilaian resiko dan pengendaliannya.
4.19 Threat: An intent of damage or injury; an indication of something impending or everything that has potency for injure or damage people, equipment, and workplace.	4.19 Ancaman: Suatu kerusakan atau luka luka ; dan merupakan indikasi dari sesuatu yg akan datang atau terjadi atau segala sesuatu yang mempunyai potensi melukai atau merusak pekerja, peralatan dan lingkungan kerja.
4.20 Normal : a condition where hazards has been predicted to arise before while activity being performed	4.20 Normal : suatu kondisi dimana ancaman sudah diperkirakan akan muncul pada saat suatu aktifitas dilakukan
4.21 Abnormal : a condition where hazards which has not predicted to arise before, has arisen while activity being performed	4.21 Abnormal : suatu kondisi dimana ancaman yang tidak diperkirakan sebelumnya muncul pada saat suatu aktifitas dilakukan
4.22 Emergency : a condition where threat or disturbance which has not predicted to arise before, has arisen while activity being performed and has increase severity quickly	4.22 Darurat : suatu kondisi dimana ancaman yang tidak diperkirakan sebelumnya muncul pada saat suatu aktifitas dilakukan dan memiliki kecepatan peningkatan keparahan yang tinggi
4.23 Risk is the chance of something happening that will have an impact on objectives or targets. It is measured in terms of likelihood and consequence and	4.23 Resiko : Resiko adalah kemungkinan kejadian yg akan mempengaruhi tujuan dan sasaran. Ini terukur melalui peluang dan akibat dan mungkin timbul dari

may arise from event, an action or from a lack of action.

4.24 Threats Control hierarchy: Options hierarchy in risk controlling. One option can be better than others or more possible to be applied.

4.25 Work instructions : Standard Work procedure to be a guideline on doing job that can avoid work accident

kegiatan, tindakan atau ketidaksesuaian tindakan.

4.24 Hirarki Pegendalian Ancaman : Urutan pilihan pilihan dalam mengendalikan resiko. Salah satu pilihan dapat saja lebih baik dari yang lainnya atau lebih dapat diterapkan.

4.25 Instruksi kerja yang aman : Cara kerja yang telah distandarkan untuk dijadikan panduan dalam melakukan pekerjaan yang dapat mencegah terjadinya kecelakaan kerja.

5 PROCEDURE

5.1 General

In order to know the potential and significant security threats the initial step is to identify all assests within Power Plant area, gas pipe line area and representatif office. Identification of assets shall involve all related functions in order to ensure that all tangible and intangible threats can be unfolded. Assests includes :

- People (Employee, tenants, guest, vendors, visitors and others directly or indirectly connected or involved with company business)
- All types of Property (building, equipments etc)
- Core business
- Networks
- Information

5.1.1 Security Risk Assessment shall be conducted/reviewed :

- Anually
- After Post Incident
- Changes in Personnel or Operations
- Changes in Legitaion

5 PROSEDUR

5.1 Umum

Untuk mengetahui ancaman keamanan yang potensial dan signifikan langkah awal nya adalah dengan melakukan identifikasi semua asset yang ada di wilayah Power Plant area, gas pipe line area dan kantor representatif. Identifikasi asset harus melibatkan semua fungsi terkait untuk memastikan bahwa semua ancaman yang nyata maupun tidak nyata dapat diungkapkan. Aset meliputi :

- Manusia (Karyawan, penyewa, tamu, vendors,dll yang secara langsung maupun tidak langsung berhubungan atau terlibat dengan bisnis perusahaan)
- Semua kekayaan yang berupa peralatan (bangunan, peralatan dll)
- Bisnis Inti
- Jaringan Kerja
- Informasi

5.1.1 Penilaian resiko keamanan in harus dilakukan atau direview:

- Per tahun
- Setelah ada Kejadian Keamanan
- Perubahan personnel dan Operasi
- Perubahan peraturan
- Ditemukan ancaman baru

- New Threats identified
- Changes in preceived level of RISK

5.1.2 After completing of assests identification, it needs to be categorized based on risk, threat and vulnerability level. Risk or threat are those incidents likely to occur at site, either due to history of such events or circumstances in the local environment. They also can be the intrinsic value of assets housed or present at a facility or event. A loss risk event can be determined through a vulnerability analysis. Vulnerability analysis should take into consideration anything that could be taken advantage of to carry out a threat. This process should highlight points of weakness and assist in the construction of a framework for subsequent analysis and countermeasures. Data source for determining threats could be criminal or non criminal (natural disaster either by man activity and natural cause) and defective impact due to activity of external party (lead to decreasing of company image by supplier, distributor, business partners)

Criminal threats includes thievery, sabotage, unhealthy business practice, deceive, hacker, stealing of information. Source of data can be but not limited to :

- Police Office (criminal data & statistics)
- Public Criminal Report from other

- Perbedaan standard resiko

5.1.2 Setelah menyelesaikan identifikasi asset, perlu mengelompokkan nya berdasarkan tingkat resiko, ancaman dan kerawanan. Resiko dan ancaman adalah merupakan kejadian yang kemungkinan terjadi di lokasi, baik berdasarkan sejarah dari kejadian kejadian yang sedemikian atau kedaaan yang ada di lingkungan lokal. Hal ini dapat juga merupakan nilai intrinsik dari aset yag dimiliki atau hadir pada fasilitas atau kejadian. Kejadian resiko kehilangan dapat ditentukan melalui analisa kerawanan. Analisa kerawanan harus mamperhatikan setiap hal yang dapat membawa keuntungan dalam menangani ancaman. Proses ini harus mampu menyingkapkan titik titik kelemahan dan membantu dalam pembangunan sebuah kerangka kerja untuk analisa yang berikutnya dan penanganannya. Sumber data untuk menentukan ancaman ancaman dapat yang bersifat kriminal atau non kriminal (bencana alam baik yang disebabkan oleh kegiatan manusia dan oleh alam) dan dampak cacat yang disebabkan oleh kegiatan dari pihak eksternal(yang menyebabkan penurunan citra perusahaan oleh pemasok, distributor, rekanan bisnis)

Ancaman kriminal meliputi, pencurian, sabotase, praktek bisnis yang tidak sehat., penipuan, hacker, pencurian informasi. Sumber data dapat berupa dan tidak terbatas pada :

- Kantor Polisi (data kriminal dan statistik)
- Laporan Kriminal Publik dari

legal agency
- Internal document of organization (Security Incident Report)
- Complaints (employee, customer, visitors etc)
- Local Intelligent agency
- Industrial Information related with crime trends
- Economic Condition (in general)
- Emerging potential crime magnet (nite club, continuous presence of vagrants etc)

5.1.3 Establish the probability of loss risk and frequency of events (F).
Frequency of events relates to the regularity of the loss event. For example, if there is the assault of patrons at a shopping mall, the frequency would be the number of times the event occurs each day that the mall is open.

Probability of loss riks is a concept based upon considerations of such past incidents, available data at working area, issues as prior incidents, environment condition, geographic location, political condition, social and economic conditions & trends, warnings or threats

The probability of loss risks are categorized as follows :
- A : Almost Certain
- B: Likely
- C: Moderate
- D: Unlikely
- E: Rare

badan hukum yg lain
- Dokumen Internal Organisasi (Laporan Insiden Keamanan)
- Keluhan Keluhan (karyawan, pelanggan, tamu dll)
- Agen inteijen local
- Informasi industri yang berhubungan dengan trend kriminal
- Kondisi Ekonomi (secara umum)
- Daya penarik kriminal yang potensial dan sedang berkembang Emerging potential crime magnet (nite club, kehadiran kaum gelandangan secara menerus dll)

5.1.3 Menetapkan kemungkian resiko kehilangan dan frekuensi kejadian (F).
Frekuensi kejadian berhubungan dengan pola/ bentuk dari kejadian kehilangan. Sebagai contoh, jika ada serangan terhadap ketertiban di shopping mall, maka frekuensi kejadiannya adalah merupakan jumlah waktu kejadian yang bisa terjadi setiap hari pada saat mall tersebut dibuka atau beroperasi.
Kemungkinan resiko kehilangan adalah merupakan suatu konsep yang berdasarkan pertimbangan pertimbangan dari kejadian masa lalu, data yang tesedia di area kerja, kondisi lingkungan, lokasi geografis, kondisi sosial ekonomi dan trendnya, peringatan atau ancaman.

Kemungkian resiko kehilangan dikelompokkan sebagai berikut :
- A : Hampir Mungkin
- B: Mungkin
- C: Moderate
- D: Tidak Mungkin
- E: Jarang

Detail description of loss risks are shown in the Appendix (Table 1)

5.1.4 **Determine the impact of the events**

The following subjects shall be considered in determining type of impacts that might be generated from certain events :

- Direct and indirect cost
- Financial
- Psychological
- Intangible loss on company assests

Severity level of impact will be evaluated and also categorized as follows :

- 1: Unknown
- 2: Relatively not Seriuos
- 3: Serious
- 4: Extremely Serious
- 5: Fatal

5.1.5 **Evaluation of Risks**

After all potential risk are identified, completed with likelihood, probability of loss risk and severity of impact (C) then they shall be evaluated based overall risk level .Types of risk level are defined as follows :

- E: Extreme Risk (need immediate actions for handling)
- H: High Risk (need attention or support from senior managements)
- M: Medium Risk (need to define the responsibility of related function)
- L: Low Risk (it can be controlled through routine procedures)

Uraian yang detil tentang resiko kehilangan ditunjukkan dalam Lampiran (Table 1)

5.1.4 **Menetapkan tingkat dampak dari suatu kejadian**

Subjek subjek berikut harus diperhatikan adalam menetapkan jenis dampak yang mungkin disebabkan dari kejadian kejadian tertentu :

- Biaya langsung dan tidak langsung
- Finansial
- Psikologi
- Kerugian yang bersifat kehilangan intangible terhadap aset perusahaan

Tingkat kerusakan dari dampak akan dievaluasi dan juga dikelompokkan sebagai berikut :

- 1: Tidak Diketahui
- 2: Secara relative tidak serius
- 3: Serius
- 4: Sangat Serious
- 5: Fatal

5.1.5 **Penilaian Resiko**

Setelah semua resiko yang potensial diidentifikasi, dilengkapi dengan kemungkinan terjadi, kemungkinan resiko kehilangan dan tingkat keparahan dampak (C) kemudian mereka harus dievaluasi berdasarkan tingkat resiko keseluruhan. Jenis jenis tingkat resiko ditetapkan sebagai berikut :

- E: Resiko Ekstrim (membutuhkan tindakan segera untuk penganganannya)
- H: Resiko Tinggi (membutuhkan perhatian dan dukungan dari manajemen senior)
- M: Resiko Medium (perlu menetapkan tanggung jawab dari fungsi fungsi terkait)
- L: Resiko Rendah (dapat dikendalikan melalui prosedur rutin)

Define the risk level by combining the level of threat probability (likelihood) with level of threat consequence (Severity) as presented on Appendices 5.1.2 and 5.1.3

Risk Score =F x C

Where ,
F = level of threat probability
C = level of threat consequence (Severity)

5.1.6 **Develop Options to mitigate risks**

In order to mitigate and prevent the loss risks need to identify availability of options through physical, procedural, logical, or related security process.

Theoritical options might be taken through :

1. Security Measures:
   - Hardware/Software
   - Policy/Procedures
   - Management practices

2. Other Means (Financial Risk) :
   - Switching of risk to assurance agency
   - Contract
   - Acceptance of residual risk.

5.1.7 **Study the feasibility of implementation of options.**

The purpose of this activity is to find out the balance between applied security strategy with business needs and psycolocigal aspects. Need to be considered that practicality on implementing the options without substantially interfering with operation

Tetapkan level resiko dengan menggabungkan kemungkinan terjadinya ancaman dengan tingkat keparahn dampak seperti yang disajikan pada Lampiran 5.1.2 and 5.1.3

Risk Score =F x C

Dimana ,
F = Tingkat kemungkinan ancaman
C = Tingkat konsekuensi ancaman (Keparahan/ Kerusakan)

5.1.6 **Mengembangkan Opsi Opsi untuk mengurangi dampak resiko**

Untuk mengurangi dampak dari resiko dan mencegah resiko kehilangan maka perlu mengidentifikasi ketersediaan pilihan pilihan berdasarkan sifat físika, prosedur, logika atau proses keamanan yang terkait.
Pilihan pilihan teoritis dapat diambil melalui :

1. Tindakan Keamanan:
   i. Hardware/Software
   ii. Kebijakan/Prosedur
   iii. Praktek Manajemen

2. Perangkat yang Lain (Resiko Keuangan) :
   - Pengalihan resiko ke pihak asuransi
   - Kontrak
   - Peneriman resiko sisa (setelah tindakan mitigasi).

5.1.7 **Mempelajari kelayakan implementasi dari pilihan pilihan .**

Maksud dari kegiatan ini adalah untuk menemukan keseimbangan antara strategi keamanan yang diterapkan dengan kebutuhan bisnis dan aspek aspek psikologi. Perlu diperhatikan kepraktisan dalam penerapan pilihan

or profitability of company.

5.1.8 **Perform a cost / benfit analysis**
The purpose of this analysis is to calculate the amount of actual cost wich impacted by implementation of selected option compared with cost implication and proportion

Result of Identification, assessment of security risks and determine control should be written and listed in Master Register of Threat and Vulnerability Identifications and Risk Assessment

5.2 **Responsibility**

5.2.1 An employee or team who has been assigned ,shall do identification and security risk assessment process in their responsible area and recommend risk control

5.2.2 Senior Security Manager shall be responsible to understand and approve threat identification, security risk assessment and risk control in their responsible area and also propose improvement or Security plan base on result of threat evalaution

5.2.3 Security Coordinator/Chief of secuirty has responsible to compile, review, analyze and propose Yearly Security Plan for each site

5.2.4 Board of Director has responsible to review and approve Yearly Security Plan and assign Project Manager for each plant

5.2.5 Contractor (BUJP) Project Manager has responsibility to develop action plan,

pilihan tanpa mempengaruhi kondisi operasi dan keuntungan perusahan secara substansial .

5.1.8 **Melakukan analisa untung/rugi**
Maksud dari analisa ini adalah untuk menghitung jumlah biaya aktual yang merupakan dampak dari implementasi pilihan yang diambil dibandingkan dengan implikasi biaya dan proporsinya.

Hasil dari identifikasi, penilaian resiko keamanan dan menetapkan pengendalian harus dituliskan di dalam Master Register of Threat and Vulnerability Identifications and Risk Assessment

5.2 **Tanggung Jawab**

5.2.1 Karyawan atau team yang telah ditunjuk harus melakukan proses identifikasi ancaman dan analisa resiko keamanan di area yang menjadi tanggung jawabnya dan mengajukan usulan pengendalian resiko

5.2.2 Manajer senior Keamanan bertanggung jawab untuk memahami dan menyetujui hasil identifikasi ancaman, analisa resiko keaman dan pengendalian resiko di area yang menjadi tanggung jawabnya serta mengajukan rencana perbaikan atau Security Plan berdasarkan hasil evaluasi ancaman .

5.2.3 Security Coordinator atau Kepala Keamanan bertanggung jawab untuk mengumpulkan, meninjau, menganalisa dan mengusulkan Security Plan tahunan untuk masing masing Lapangan.

5.2.4 Dewan Direksi bertanggung jawab untuk meninjau dan menyetujui Security Plan tahunan serta mengangkat Project Manager di masing – masing lokasi.

develop team and report the progress in every month to Security Coordinator and / or Chief of Security

5.3 **Security Plan & Program**

5.3.1 Result of risk should be compiled by, reviewed by Security Coordinator/Chief of Security and approved by Manager using Risk Control Register Form and then proposed it into Site Security Plan via Plant Review Meeting with considering some aspect as follow :

- Legal
- Availability of technology
- Finance
- Business operation
- Risk level

5.3.2 Security Contractor Project Manager and due date should be fixed for each Plant Security Plan. In addition Security Ocjective & Target and Security Program shall be developed in each function.

5.3.3 Security Contractor Project Manager who has been assigned for Plant Security Plan should make team and develop activity plan

5.3.4 All of Site Security Plan should be included to company business risk map

5.3.5 Progress implementation of Plant Security Plan should be monitored by Security Coordinator and / or Security authority to be reported to Top Management .

5.2.5 BUJP atau Kontraktor Pengamanan Project bertanggung jawab untuk mengembangkan rencana kerja, menentukan team dan melaporkan kemajuan setiap bulan kepada Security Coordinator dan / atau Kepala Keamanan (internal)

5.3 **Security Plan & Program**

5.3.1 Hasil dari penilaian resiko harus dirangkum, ditinjau oleh security coordinator/Kepala keamanan dan disetujui oleh Manager dengan menggunakan Formulir standar Register Kontrol Resiko untuk kemudian diusulkan untuk dibuatkan Site Security Plan melalui Plant Review Meeting dengan mempertimbangkan hal-hal sebagai berikut :

- Legal
- Ketersediaan Teknologi
- Keuangan
- Operasi Bisnis
- Tingkat resiko

5.3.2 Project Manager dan target rencana pencapaian harus ditentukan untuk setiap Plant Security Plan. Disamping itu Tujuan dan Sasaran Keamanan serta Program Keamanan harus dikembangkan di setiap fungsi yg terkait.

5.3.3 Project Manager yang telah ditunjuk untuk Plant Security Plan diharuskan membentuk team dan menyusun rencana kerja

5.3.4 Seluruh Rancangan Pengamanan harus dimasukkan dalam business risk map Perusahaan

5.3.5 Kemajuan pelaksanaan Plant Security Plan harus dimonitor oleh Security Coordinator dan / atau Otoritas Security

5.3.6 A Security Plan could be closed if low risk level has been got from re-risk assessment or in technic and administration, threat can not be eliminated

6 RECORD

6.1 Master Register of Threat Identifications and Risk Assessment

6.2 Security Improvement Form

7. ATTACHMENT

7.1 Probability/Likelihood Criteria
7.2 Impack Criteria
7.3 Risk Level Category
7.4 Risk Level Matrix
7.5 Security Threat and Risk Evaluation
7.6 Flow Chart

untuk kemudian dilaporkan kepada Manajemen Puncak.

5.3.6 Suatu Security Plan dinyatakan telah selesai jika dari hasil penilaian resiko ulang diperoleh hasil tingkat resiko yang rendah atau secara teknis dan administrasi sudah tidak mungkin diturunkan lagi tingkat ancamannya

6 REKAMAN

6.1 Formulir Standar Register Induk Identifikasi Ancaman dan Penilaian Resiko

6.2 Formulir standar Rencana Perbaikan Security

7 LAMPIRAN

7.1 Kriteria untuk kemungkinan
7.2 Kriteria untuk akibat
7.3 Pengelompokan Tingkat Resiko
7.4 Matriks Tingkat Resiko
7.5 Security Threat and Risk Asessment
7.6 Flow Chart

8 Summary Of Revision

Date	Rev.	Section	Description	Approval

INTENTIONALY LEFT BLANK

Appendix 7.1 Probability/Likelihood Criteria

Criteria	Desription	Level (Attribute)
Almost Certain Hampir Pasti	*It is possible happened / it was predicted will be happened in any chance* Sangat mungkin akan terjadi / hampir dipastikan akan terjadi pada semua kesempatan	A
Quite Possible (Likely) Mungkin Terjadi	*Perhaps will be happened in all conditions* Mungkin akan terjadi pada hampir semua kondisi	B
Unusual but possible (Moderate) Tidak biasa namun bisa terjadi	*Un usual not happened but still has possibility to happen in every time* Biasanya tidak terjadi namun masih ada kemungkinan untuk dapat terjadi tiap saat	C
Unlikely Kecil kemungkinannya	*An accident might be happened in many specific conditions, but the probability is too small.* Suatu kejadian mungkin terjadi pada beberapa kondisi tertentu, namun kecil kemungkinannya untuk terjadi	D
Rare Jarang sekali	*An accident could be happened in a certain/ extremely condition, after several years.* Suatu indiden mungkin dapat terjadi pada suatu kondisi yang khusus/luar biasa, setelah bertahun-tahun	E

Appendix 7.2 Severity level

Criteria / Kriteria	Description	Level (Attribute)
Fatal Fatal	*The lost can cause recapitalization or long period of discontinuity* Kehilangan yang dapat mengakibatkan rekapitalisasi atau ketidakberlangsungan jangka panjang	1
Very Serious Sangat Serius	*The lost which can cause significant changes on investment policy and generating great impact on stability.* Kehilangan yang dapat mengakibatkan perubahan besar dalam kebijakan investasi dan berdampak besar pada keseimbangan	2
Serious Serius	*The lost wich cause very significant impact on revenue and require more attention from senior executive of management* Kehilangan yang sangat berdampak pada pendapatan dan memerlukan perhation manajemen senior eksekutif	3
Relatively not serious Relatif tidak serius	*The lost which is budgeted in operational expenditure during that tinancial period* Kehilangan yang akan dianggarkan pada pengeluaran operasional normal selama periode masih berlangsung	4
Unknown Tidak Diketahui	*The lost has been replaced along with replacement for the four priorities, jus before determining its priority.* Sebelum prioritas ditetapkan, kehilangan telah digantikan bersamaan dengan pergantian keempat prioritas lainnya.	5

Appendix 7.3 Risk Level Category

RISK Category	Criteria	Note
E	Very High/ Sangat Tinggi	*this risk require immediate corrective action* resiko ini memerlukan penanganan/tindakan segera
H	High / Tinggi	*Need monitoring form top management and immediately action should be done* Perlu mendapat perhatian dari pihak Manajemen Puncak dan tindakan perbaikan segera dilakukan
M	Medium / Menengah	*Corrective action plan can be scheduled later and improvement can be taken from current procedure* Tindakan perbaikan dapat dijadwalkan kemudian dan penanganan cukup dilakukan dengan prosedur yang ada
L	Low / Rendah	*Risk can be acceptable, and the risk can be controlled by routine procedure* Resiko dapat diterima, dan resiko dapat dikendalikan dengan prosedur rutin.

Appendix 7.4 Risk Level Determination or Matrix

Probability	Severity				
	E	D	C	B	A
I	*H*	*H*	*E*	*E*	*E*
II	*M*	*H*	*H*	*E*	*E*
III	*L*	*M*	*H*	*E*	*E*
IV	*L*	*L*	*M*	*H*	*E*
V	*L*	*L*	*M*	*H*	*H*

Attachment 7.5 Security Threat and Risk Evaluation

No.	Activity	Asset	Critical Function	Threat	Control	Vulnerability	Likelihood	Severity	Risk Level
	1	2	3	4	5	6	7	8	9 = 7 x 8
	Type of Activity	*Asset Name*	*What is the critical function?*	*What is the threat?*	*What is current control on threat?*	*What is potential threat over the current control?*	*What is the probalility of incident?*	*Severity of threat if it happened.*	*The risk level of incident*
				-					M

Attachment 7.6 FLOW CHART

Flowchart - Simplified flow chart of Threat Identifications and Risk Assessment and Realization Plan

Area : security Management System	Procces Owner : MRPR
Title : Diagram Alur Identivikasi Dan penilaian Terhadap Ancaman Dan Resiko Keamanan	Created by :MRPR
Description : Untuk Penjelasan Proses Identifikasi Dan Penilaian Terhadap Potensi Bahaya,Ancaman Yang menimbulkan resiko keamanan	Approved by :
	Approved daate :