CONTROL SYSTEM CYBERSECURITY DESIGN CRITERIA

ENGINEERING TECHNICAL STANDARDS & PROCEDURES

PT KILANG PERTAMINA INTERNASIONAL

DIREKTORAT PROYEK INFRASTRUKTUR

01	Issued For Record	10/22	YPJ/ASY	JMS	ASR	RMD	BAP
00	Issued For Record	12/21	YPJ/ASY	JMS	ASR	RMD	BAP
Rev.	Description	Date	Prepared by	Checked by	Verified by	Validated by	Approved By

REVISION HISTORY
RIWAYAT REVISI

Page / Section *Hal. / Bagian*	Date *Tanggal*	Description *Deskripsi*	Revised by *Direvisi oleh*
1-69	07/10/22	Add: Content translation in Bahasa *Penambahan: Penerjemahan konten dalam Bahasa*	**Team Comittee**
1-69	07/10/22	Change: Format and document numbering related to restructuring of Pertamina *Perubahan: format dan penomoran dokumen terkait restrukturisasi Pertamina*	**Team Comittee**
4.	09 Aug 21	Add sentence: "Contractor shall not modify existing ICSS cyber security design, unless specified by OWNER." *Tambahkan kalimat: Kontraktor tidak harus memodifikasi desain cyber security ICSS eksisting tanpa diminta oleh OWNER.*	**TEAM COMITTE**
6.3	09 Aug 21	Add sentence: "Penetration test and vulnerability test shall be done during SAT. Contractor shall ensure that after the pen-test (penetration test) and vulnerability test all Pertamina Corporate software and network stay functioning normally without being impacted by the testing activities." Tambahkan kalimat: Penetration test dan Vulnerability test harus dilakukan selama SAT. Kontraktor harus menjamin agar setelah dilakukan pen-test (penetration test) dan vulnerability test seluruh software dan jaringan di Pertamina Corporate tetap berfungsi normal tanpa terpengaruh oleh aktifitas testing.	**TEAM COMITTE**
		Add sentence: "In designing IPS, Vendor shall guarantee the performance of both existing & new network are not degraded. Tambahkan kalimat: Dalam desain IPS, Vendor harus memberikan garansi performance terhadap jaringan lama dan baru tidak menjadi berkurang.	**TEAM COMITTE**
8.1	09 Aug 21	Add sentence: "In designing the heartbeat signals, Vendor shall determine and set the time of communication timeout that shall not degrading the	**TEAM COMITTE**

		performance of ICSS." Penambahan: Dalam membuat desain heartbeat signals, Vendor harus menentukan dan melakukan setting waktu timeout komunikasi sehingga tidak akan mengurangi performance dari ICSS.	
8.10	09 Aug 21	Replace "(6.0 as of 2016)" with "version 7 or latest" Perubahan (6.0 dari 2016) dengan (versi 7 atau terbaru).	**TEAM COMITTE**
1	16 Des 21	Revise "…Project of Refinery & Petrochemical Megaproject Directorate" to be "….Project of Kilang Pertamina Internasional" Perubahan :".. Project of Refinery & Petrochemical Mega Project Directorat menjadi Kilang Pertamina International	**TEAM COMITTE**
2	16 Des 21	Revise "…between Pertamina and/or Contractor and Vendors" to be "….between Kilang Pertamina Internasional and/or Contractor and Vendors." Perubahan: " .. antara Pertamina dan/atau Kontraktor dan Vendor menjadi ".. antara Kilang Pertamina International dan/atau Kontraktor dan Vendor."	**TEAM COMITTE**

TABLE OF CONTENTS

DAFTAR ISI

1. INTRODUCTION

1.1 This document defines cybersecurity guidelines for Instruments and Control Systems interfaces that will be managed by OWNER, PMT, PIT, EPC Contractors, Vendors and Third Parties for the Project of Kilang Pertamina Internasional

1. PENGANTAR

1.1 Dokumen ini mendefinisikan pedoman keamanan siber untuk antarmuka dari Instrumen dan Sistem Kontrol yang akan dikelola oleh PEMILIK, PMT, PIT, Kontraktor EPC, Vendor dan Pihak Ketiga untuk Proyek Kilang Pertamina Internasional

2. SCOPE

2.1 This document defines the overall Integrated Control and Safety System (ICSS) Cybersecurity Philosophy for the project. Although this document is mainly applicable for the EPC phase, it will also be applicable for FEED phase where multiple FEED Contractors/3rd Parties are involved.

The cybersecurity philosophy for the business network is not part of the scope of this document. This philosophy is also applicable for all electrical switches containing embedded software that allows them to be controlled via computer based applications (and/or via a web page).

This document does not cover the Instruments interfaces with external parties such as permitting authorities, local authorities etc. This document also does not cover any interfaces between Kilang Pertamina Internasional and/or Contractor and Vendors. Any contradiction between this document and the Contractor's scope of work shall be brought to the attention of the PMT.

Cybersecurity is the responsibility of each and every contractor and vendor. There shall be one point of reference contractor who shall coordinate and implement the overall cybersecurity strategies for the whole network, and it shall be the ICSS

2. LINGKUP

2.1 Dokumen ini mendefinisikan Filosofi Keamanan Siber dari *Integrated Control and Safety System (ICSS)* secara keseluruhan dalam suatu proyek. Dokumen ini berlaku untuk fase EPC dan fase FEED di mana banyak Kontraktor FEED/Pihak Ketiga terlibat.

Filosofi keamanan siber untuk jaringan bisnis bukan bagian dari cakupan dokumen ini. Filosofi ini juga berlaku untuk semua *switch switch* elektrikal yang berisi perangkat lunak bawaan yang memungkinkan untuk dikendalikan melalui aplikasi berbasis komputer (dan/atau melalui halaman *web*).

Dokumen ini tidak mencakup antarmuka Instrumen dengan pihak eksternal seperti otoritas perijinan, otoritas lokal, dll. Dokumen ini juga tidak mencakup antarmuka antara Kilang Pertamina Internasional dan/atau Kontraktor dan Vendor. Setiap kontradiksi antara dokumen ini dan ruang lingkup pekerjaan Kontraktor harus menjadi perhatian PMT.

Keamanan siber merupakan tanggung jawab dari setiap kontraktor dan vendor, dimana akan menjadi satu referensi yang digunakan oleh kontraktor untuk melakukan koordinasi dan implementasi keseluruhan keamanan siber dari seluruh jaringan, dan

Contractor. All contractors shall support the ICSS contractor with all necessary hardware, software and documents for the overall cybersecurity strategy for the whole (all EPC) new plant, with possibility for a later upgrade of the existing sections of the plant.

Contractor shall not modify existing ICSS cyber security design, unless specified by OWNER.

ini harus menjadi tanggung jawab kontraktor ICSS. Seluruh kontraktor harus mendukung kontraktor ICSS dari setiap perangkat keras, perangkat lunak dan dokumen yang dipasoknya untuk mendukung keseluruhan strategi keamanan siber baik untuk kilang baru maupun peningkatan kilang eksisting.

Kontraktor tidak boleh melakukan modifikasi keamanan siber eksisting tanpa diminta oleh PEMILIK.

3. CONFLICTS AND DEVIATIONS

3.1 Any conflicts between this standard and other applicable Engineering Technical Standards & Procedures (ETSP), or OWNER standard, codes, and forms shall be resolved in writing by OWNER.

3.2 All direct requests to deviate from this standard (ETSP) in writing to OWNER, who shall follow internal OWNER procedure and forward such requests to OWNER for approval.

3. KONFLIK DAN DEVIASI

3.1 Apabila terdapat konflik antara standar ini dengan *Engineering Technical Standards & Procedures* (ETSP) yang berlaku lainnya, atau standar PEMILIK, kode dan formulir, maka harus diselesaikan secara tertulis oleh PEMILIK.

3.2 Semua permintaan penggunaan standar yang berbeda dari standar ini (ETSP), harus diajukan kepada PEMILIK secara tertulis dengan mengikuti prosedur *internal* PEMILIK untuk mendapatkan persetujuan.

4. ABBREVIATIONS

4.1 Abbreviations used for this specification shall have the following definitions:

AIC	Availability, Integrity, and Confidentiality
BIOS	Basic Input Output System
BPCS	Basic Process Control System
CCTV	Closed Circuit Television
CIA	Confidentiality, Integrity, and Availability
DMZ	De-Militarized Zone (Architectural Level 3.5)
DOR	Division of Responsibility

4. SINGKATAN

4.1 Singkatan yang digunakan pada spesifikasi ini harus memiliki definisi sebagai berikut:

AIC	*Availability, Integrity, and Confidentiality*
BIOS	*Basic `Input Output System*
BPCS	*Basic Process Control System*
CCTV	*Closed Circuit Television*
CIA	*Confidentiality, Integrity, and Availability*
DMZ	*De-Militarized Zone (Architectural Level 3.5)*
DOR	*Division of Responsibility*

EPC	Engineering Procurement and Construction	EPC	*Engineering Procurement and Construction*
EWS	Engineering Work Station	EWS	*Engineering Work Station*
FAT	Field Acceptance Test	FAT	*Field Acceptance Test*
FEED	Front End Engineering Design	FEED	*Front End Engineering Design*
GPS	Global Positioning Satellite	GPS	*Global Positioning Satellite*
HMI	Human Machine Interface	HMI	*Human Machine Interface*
ICSS	Integrated Control and Safety System	ICSS	*Integrated Control and Safety System*
IP	Interface Point	IP	*Interface Point*
IQ	Interface Query	IQ	*Interface Query*
ISH	Instrument Satellite House	ISH	*Instrument Satellite House*
LAN	Local Area Network	LAN	*Local Area Network*
OWNER	PT. PERTAMINA (Persero)	OWNER	*PT. PERTAMINA (Persero)*
PCN	Process Control Network	PCN	*Process Control Network*
PESG	PERTAMINA Engineering Services Group	PESG	*PERTAMINA Engineering Services Group*
PLC	Programmable Logic Controller	PLC	*Programmable Logic Controller*
PMT	Project Management Team	PMT	*Project Management Team*
RDMP	Refinery Development Master Plan	RDMP	*Refinery Development Master Plan*
SAT	Site Acceptance Test	SAT	*Site Acceptance Test*
PIT	Project integration Team	PIT	*Project integration Team*
SPI	Smartplant Instrumentation	SPI	*Smartplant Instrumentation*
STG	Steam Turbine Generator	STG	*Steam Turbine Generator*
TCP/IP	Transmission Control Protocol / Internet Protocol	TCP/IP	*Transmission Control Protocol / Internet Protocol*
UCP	Unit Control Panel	UCP	*Unit Control Panel*
Vendor	3^{d} party who provides service or equipment, as contracted by an EPC or major contractor; or the ICSS contractor.	Vendor	*3^{d} party who provides service or equipment, as contracted by an EPC or major contractor; or the ICSS contractor.*

5. DEFINITIONS

5. DEFINISI

5.1 The following words shall have these special meanings when used herein:

OWNER	Owner of the Plant is defined as PT Kilang Pertamina Internasional
CONTRACTOR/ CONSULTANT	Defined as the Organization to which PT Kilang Pertamina Internasional assign the work
Vendor	3d party who provides service or equipment, as contracted by an EPC or major contractor; or the ICSS contractor.
shall	Indicates that the statement is mandatory
should	Indicates a recommendation

6. CODES AND STANDARDS

The following Codes, Standard and Specifications apply to this specification. When an edition date is not indicated for a code or standard or any update in codes and standards in this specification document, the latest edition and addendum in force at the time of purchase shall apply. Material & equipment shall be as a specification or an equal approved by OWNER.

6.1 Reference Documents

ISA/IEC 62443	Security for Industrial Automation and Control Systems.
DHS	Cyber Security

5.1 Penggunaan kata-kata berikut harus memiliki arti khusus sebagai berikut:

PEMILIK	Pemilik dari Kilang didefinisikan sebagai PT Kilang Pertamina Internasional
KONTRAKTOR/ KONSULTAN	Didefinisikan sebagai Organisasi yang ditunjuk oleh PT Kilang Pertamina Internasional untuk melakukan suatu pekerjaan
Vendor	Pihak ketiga yang menyediakan layanan atau peralatan sebagaimana dikontrak oleh EPC atau kontraktor utama atau kontraktor ICSS.
shall	Menunjukkan bahwa pernyataan itu wajib
should	Menunjukkan rekomendasi

6. KODE DAN STANDAR

Kode, standar, dan spesifikasi berikut berlaku untuk spesifikasi ini. Kode dan standar harus menggunakan edisi yang terbaru atau edisi yang berlaku pada saat pembelian. *Material* & peralatan harus sesuai spesifikasi atau setara dengan yang disetujui oleh PEMILIK.

6.1 Dokumen Referensi

ISA/IEC 62443	*Security for Industrial Automation and Control Systems.*
DHS	*Cyber Security*

Procurement Language for Control Systems issued September 2009	*Procurement Language for Control Systems issued September 2009*
Framework for Improving Critical Infrastructure Cybersecurity – Version 1.0 by the National Institute of Standards and Technology (NIST).	Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritikal – Versi 1.0 oleh *National Institute of Standards and Technology (NIST).*

7. SYSTEM COMPONENTS

The general priority of the of the ICSS security system is to maintain the availability of all its components, the integrity of the equipment and processes under its control, and, to a lesser degree, protect the data from unauthorized access (confidentiality). That is commonly known as AIC.

In traditional information security networks the priorities are often inverted as those for the industrial control systems, where protection of the data is of the upmost importance. In industrial control system, the data is often raw and requires analysis within the context of the specific plant and operation to be of value. That is commonly known as CIA.

The project shall follow the concept of “Defense-In-Depth” for the design and implementation of its cybersecurity system, which includes applying different protection layers that will go from restricting physical access to the assets to providing information technology protection systems like firewalls, intrusion prevention systems, antivirus, etc.

The “Defense-In-Depth” concept includes the analysis and design of the system to protect against external and internal,

7. KOMPONEN SISTEM

Prioritas umum dari sistem keamanan ICSS adalah untuk melindungi data terhadap otorisasi akses (kerahasiaan) untuk seluruh komponen yang terintegrasi dari seluruh peralatan dan proses yang dikontrol dan juga pada tingkat yang lebih rendah. Hal ini secara umum disebut sebagai *AIC*.

Dalam informasi keamanan jaringan tradisional terjadi prioritas sering terbalik dengan yang ada dalam sistem kontrol industri, dimana keamanan dari data adalah yang terpenting. Dalam sistem kontrol industri, data sering merupakan data mentah dan membutuhkan analisa didalam keterkaitannya dengan kilang secara spesifik dan operasinya kedalam nilai tertentu. Hal ini secara umum disebut sebagai *CIA.*

Proyek harus mengikuti konsep *“Defense-In-Depth” (DID)* untuk desain dan implementasi dari sistem keamanan siber, yang melibatkan penggunaan lapisan lapisan proteksi yang berbeda mulai dari pembatasan akses fisik aset sampai menyediakan sistem proteksi teknologi informasi seperti *firewalls*, sistem pencegahan intrusi , *antivirus*, dll.

Konsep DID termasuk didalamnya analisa dan desain dari sistem untuk proteksi terhadap serangan dan ancaman dari

intentional and unintentional, attacks and threats.

7.1 Access Control

The overall physical access to the facility will be protected by a fence, gates with access control systems, security personnel, and a CCTV system that will allow the monitoring of the perimeter of the plant.

Inside the plant, there will be restriction of access to control and server centers to allow only authorized personnel admittance to those areas. Workstations, servers, and network equipment will be located in locked cabinets with KVM extensions.

In addition, two-factor user authentication will be implemented on the workstations to allow logging-in. Different levels of access, such as, Operator, Engineer, Administrator, etc., will be defined on the operator workstations, engineering workstations, and servers, as applicable.

7.2 Integration to 3rd Party Control Systems

Integration of the 3rd party package equipment's PLCs to the Basic Process Control System (BPCS) will include the use of firewalls that will be configured to allow only Modbus TCP/IP communication. All other functionality will be blocked.

Firewall factory pre-configured devices specifically designed and tested to interface to the specific BPCS are preferred.

7.3 Intrusion Prevention System (IPS)

An Intrusion Prevention System will be installed on the Level 3 network to detect unauthorized access to the network and to prevent vulnerability exploits by taking

external maupun internal baik yang mempunyai tujuan tertentu maupun yang tidak.

7.1 Kontrol Akses

Keseluruhan akses fisik ke fasilitas kilang akan dilindungi seperti dengan pagar, pintu masuk yang dilengkapi dengan sistem kontrol akses, petugas keamanan dan sistem CCTV untuk memonitor pagar kilang.

Didalam kilang akan dilengkapi dengan fasilitas pembatasan akses masuk ke ruang pusat control dan server sehingga hanya personel yang mempunyai otorisasi saja yang bisa masuk. *Workstation, server* dan peralatan jaringan akan ditempatkan di suatu kabinet lengkap dengan fasilitas kunci dan *KVM*.

Sebagai tambahan, untuk mengijinkan *log-in* ke *workstation* menggunakan otentikasi pengguna dua faktor. Perbedaan tingkatan akses, seperti Operator, Engineer, Administrator dll akan di definisikan didalam *workstation, engineering workstation* dan *serve*r sejauh yang dapat digunakan.

7.2 Integrasi dengan Sistem Kontrol Pihak Ketiga

Integrasi dari paket peralatan paket berbasis PLC ke BPCS akan melibatkan penggunaan *firewall* yang akan dikonfigurasi hanya untuk mengijinkan Komunikasi dengan *Modbus TCP/IP*.

Firewall yang sudah di konfigurasi awal di pabrik secara khusus di desain dan di tes untuk melakukan antarmuka dengan *BPCS* tertentu.

7.3 Sistem Pencegahan Intrusi *(IPS)*

IPS akan dipasang di jaringan level 3 yang berfungsi untuk mendeteksi akses dari yang tidak punya otorisasi ke jaringan dan untuk mencegah adanya celah keamanan dengan

actions such as dropping the malicious packets detected, blocking traffic from the source address, etc.

The IPS will also notify the network administrators of the intrusion.

Penetration test and vulnerability test shall be done during SAT. Contractor shall ensure that after the pen-test (penetration test) and vulnerability test all Pertamina Corporate software and network stay functioning normally without being impacted by the testing activities.

In designing IPS, Vendor shall guarantee the performance of both existing & new network are not degraded.

7.4 Network Asset Manager

A Network Asset Manager will be installed on the Level 3 network to allow the deployment of software patches and updates to the workstations and servers connected to the network as well as perform the regular asset administration functions like software and hardware inventory.

7.5 Level 3 Router

A router with Access Control List (ACL) will be installed as interface between Level 4, Level 3 and Level 3.5 or De-Militarized Zone (DMZ) to allow traffic of specific protocols and functions between the levels, such as, time synchronization, interface to the business data shadow historian, back up services, and antivirus protection.

7.6 Antivirus Server

An Antivirus Server will be installed on the DMZ to allow the deployment of antivirus software and updated virus definition files to all of the workstations and servers on the Level 3 network and below.

mengambil langkah seperti mendeteksi paket jahat, melakukan pemblokiran lalu lintas dari alamat sumber, dll.

IPS juga akan memberikan notifikasi adanya intrusi ke administrator jaringan.

Uji penetrasi dan uji kerentanan harus dilakukan selama *SAT*. Kontraktor harus memastikan bahwa setelah uji penetrasi dan uji kerentanan semua perangkat lunak dan jaringan Perusahaan Pertamina tetap berfungsi normal tanpa terpengaruh oleh akibat adanya kegiatan pengujian.

Dalam mendesain *IPS*, *Vendor* harus menjamin kinerja jaringan baik yang sudah ada maupun yang baru tidak akan mengalami penurunan.

7.4 Manajer Aset Jaringan

Software Network Asset Manager akan dipasang di jaringan Level 3 untuk memungkinkan pengiriman *patch* dan pembaruan perangkat lunak ke *workstation* dan *server* yang terhubung ke jaringan serta melakukan fungsi administrasi aset secara rutin seperti melakukaqn inventarisasi perangkat lunak dan perangkat keras.

7.5 *Router* Level 3

Router dengan *Access Control List (ACL)* akan dipasang sebagai antarmuka antara Level 4, Level 3 dan Level 3.5 atau *De-Militarized Zone (DMZ)* untuk memungkinkan lalu lintas protokol dan fungsi tertentu antar level, seperti, sinkronisasi waktu, antarmuka ke *shadow historian* data bisnis, layanan *back up*, dan proteksi *antivirus.*

7.6 *Server Antivirus*

Server Antivirus akan diinstal pada *DMZ* untuk memungkinkan penyebaran perangkat lunak *antivirus* dan file definisi *virus* yang diperbarui ke semua *workstation* dan *server* di jaringan Level 3 dan di

7.7 Back Up Server

A Backup Servers cluster will be installed on Level 3 to backup all servers and workstations without exception, as a prevention for any potential failure. Such failure can be an act of god, a virus attack, or any potential act that would require rebuilding of the failed device.

There shall be on-site and off-site backups per a predetermined “backup plan” and a “disaster recovery plan”.

A separate Back Up Server will be installed on the DMZ to automatically capture and maintain a back-up of the configuration and the data of the servers on this level, to help restore any machine as part of the disaster recovery plan.

7.8 One-Way Gateway/Firewall

A one-way gateway or a firewall shall be installed between the DMZ and the Level 4 network to allow read-only information traffic from the process control network to the business network. No direct traffic from the business network to process control network shall be permitted.

7.9 Wireless Network for Procesc Control

Wireless instrumentation, when used, will be deployed throughout the process areas, at the Level 0 of the network, for monitoring functions as part of the normal tasks of the BPCS. The wireless instrumentation and gateways technology include out-of-the-box security features to prevent unauthorized

bawahnya.

7.7 *Server* Cadangan

Sekelompok *Server* Cadangan akan dipasang di jaringan Level 3 untuk mencadangkan semua *server* dan *workstation*, sebagai pencegahan untuk potensi kegagalan. Kegagalan tersebut dapat berupa hal yang tidak diketahui penyebabnya, serangan virus, atau tindakan potensial apa pun yang memerlukan perbaikan kembali perangkat yang gagal.

Harus ada pencadangan di lokasi dan di luar lokasi sesuai dengan “rencana pencadangan” dan “rencana pemulihan dari bencana” yang telah ditentukan sebelumnya.

Server Cadangan terpisah akan dipasang pada *DMZ* yang secara otomatis akan menangkap dan memelihara cadangan konfigurasi dan data pada tingkat server, untuk membantu memulihkan mesin sebagai bagian dari rencana pemulihan dari bencana.

7.8 *Gateway / Firewall* satu arah

Gateway atau *firewall* satu arah harus dipasang antara DMZ dan jaringan Level 4 untuk memungkinkan lalu lintas informasi yang terbatas hanya baca (*read only*) dari jaringan kontrol proses ke jaringan bisnis. Tidak ada lalu lintas langsung dari jaringan bisnis ke jaringan kontrol proses yang diizinkan.

7.9 Jaringan nirkabel untuk Kontrol Proses

Dalam instrumentasi nirkabel, data akan disebarkan ke seluruh area proses, di Level 0 jaringan, untuk fungsi pemantauan sebagai bagian dari tugas normal *BPCS*. Teknologi instrumentasi dan *gateway* nirkabel mencakup fitur keamanan siap pakai untuk mencegah akses yang tidak sah. Beberapa

access. Some of the features are: 128-bit encryption, individual session keys, unique join keys, secure sockets layer (SSL) enable TCP/IP communication, secured certificates, etc.

7.10 Other Protection Measures

Other protection measures will be implemented by means of configuration of the workstations and servers. They include but are not limited to:

- IP Segregation (VLAN)
- Blocking of USB ports: prevents USB devices to interface with the workstation avoiding potential introduction of viruses, spyware, malware, as well as protecting the integrity of the data.
- Whitelisting: allows only authorized applications to run on the workstations. The applicability of this method will be confirmed with the ICSS supplier to ensure that it does not adversely affect the ability of the Operators, in any way, to control the process or that it will not disabled any functionality normally available to them.

7.11 Procedures

Once the system is in place, as part of commissioning, the following procedures – at a minimum – shall be turned over to the OWNER, to maintain the protection of the network:

- Disaster Recovery Plan: Outlines the procedures to restore the functionality of any part of the network in the event of a catastrophic event, which go from the simple hardware failure of a workstation to a natural disaster with

fiturnya adalah: enkripsi 128-bit, kunci sesi individu, kunci gabungan unik, lapisan soket aman (*SSL*) mengaktifkan komunikasi *TCP/IP*, sertifikat aman, dll.

7.10 Tindakan proteksi lainnya

Tindakan proteksi lainnya akan diterapkan melalui konfigurasi *workstation* dan *server*. Mereka termasuk tetapi tidak terbatas pada:

- Segregrasi *IP (VLAN)*
- Pemblokiran port USB: mencegah perangkat USB untuk berinteraksi dengan *workstation* untuk menghindari kemungkinan masuknya *virus, spyware, malware,* serta melindungi integritas data.
- *Whitelisting*: hanya mengizinkan aplikasi yang diotorisasi untuk berjalan di *workstation*. Penerapan metode ini akan dikonfirmasikan dengan vendor *ICSS* untuk memastikan bahwa metode ini tidak mempengaruhi kemampuan Operator dengan cara apa pun untuk mengontrol proses dan metode tersebut tidak akan dapat menonaktifkan suatu fungsi apa pun yang tersedia bagi mereka.

7.11 Prosedur

Setelah sistem terpasang, sebagai bagian dari *commissioning*, untuk menjaga prosedur proteksi jaringan berikut – minimal – harus diserahkan kepada PEMILIK,:

- Rencana Pemulihan Bencana: Menguraikan prosedur untuk memulihkan fungsi suatu bagian dari jaringan jika terjadi bencana, yang dimulai dari kegagalan perangkat keras sederhana pada *workstation* hingga bencana alam dengan dampak

a much wider impact.

- Patch Management Plan: Defines the procedures and requirements, including testing, to deploy software patches and updates.
- Network Asset Management: Defines the network management tasks and procedures, such as, antivirus scanning policies, printer management, hardware and software inventory, etc.
- Security related organization and policies: Includes the organization of security related responsibilities, training, awareness, human resource issues and legal related issues and policies.
- Security assessments and reviews: Includes the activities to verify that the required protection targets are achieved on the solution design, implementation, operation and maintenance.
- Change management: Includes the procedures for adding, removing, upgrading / updating and configuring assets, including the approval procedures, the configuration of assets includes in particular active / passive functions and services as well as open and closed ports.

8. INTERFACE PARTIES RESPONSIBILITIES

8.1 Interface Parties

The different parties involved in the interfaces are referred to, as:

yang jauh lebih luas.

- Rencana Manajemen *Patch*: Mendefinisikan prosedur dan persyaratan, termasuk pengujian, untuk mendistribusikan *patch* dan pembaruan perangkat lunak.
- Manajemen Aset Jaringan: Mendefinisikan tugas dan prosedur manajemen jaringan, seperti, kebijakan pemindaian *antivirus*, manajemen printer, inventaris perangkat keras dan perangkat lunak, dll.
- Organisasi dan kebijakan terkait keamanan: Termasuk organisasi yang bertanggung jawab terkait keamanan, pelatihan, kesadaran, masalah sumber daya manusia, serta masalah dan kebijakan terkait hukum.
- Penilaian dan tinjauan keamanan: Mencakup kegiatan untuk memverifikasi bahwa target proteksi yang diperlukan tercapai pada desain solusi, implementasi, operasi dan pemeliharaan.
- Manajemen perubahan: Meliputi prosedur penambahan, penghapusan, peningkatan/pemutakhiran dan konfigurasi aset, termasuk prosedur persetujuan, konfigurasi aset mencakup khususnya fungsi dan layanan aktif/pasif serta port terbuka dan tertutup.

8. PIHAK ANTARMUKA DAN TANGGUNG JAWAB

8.1 Pihak Antarmuka

Berbagai pihak yang terlibat dalam antarmuka disebut, sebagai:

- Os and Us Contractor
- ISBL Contractor
- Package Vendor(s)
- ICSS Contractor: Instrument Automation Integration and Information System
- PMT/PIT
- OWNER

All the communication related to interfaces shall be through PMT. The responsibilites are defined as following below:

8.1.1. ICSS Contractor

ICSS Contractor is responsible for the ICSS and all the associated interfaces to it, telecommunication and operator training's simulator.

8.1.2. Os & Us Contractor

Os&Us Contractor is the contractor responsible for the Os & Us units.

8.1.3. ISBL Contractor

ISBL Contractor is responsible for a process unit or group of process units. These process units could be licensor units or non-licensor units. This will also include CDU revamp.

8.1.4. PMT/PIT

Refer to the Interface Management document for definition and role of PMT and PIT.

Os&Us Contractor, ISBL Contractors and ICSS Contractor shall exchange design information, calculations and drawings via Interface Query (IQ) and coordination meetings in a timely manner to allow both to execute

- Kontraktor *Os* dan *Us*
- Kontraktor *ISBL*
- Vendor Sistem Paket
- Kontraktor *ICSS*: Integrasi Instrumen dan sistem informasi.
- *PMT/PIT*
- Pemilik

Semua komunikasi yang terkait dengan antarmuka harus melalui *PMT*.

8.1.1. Kontraktor *ICSS*

Kontraktor *ICSS* bertanggung jawab atas *ICSS* dan semua antarmuka yang terkait, telekomunikasi dan simulator pelatihan operator.

8.1.2. Kontraktor *Os* dan *Us*

Kontraktor Os&Us adalah kontraktor yag bertanggung jawab terhadap unit *Os & Us*.

8.1.3. Kontraktor *ISBL*

Kontraktor ISBL bertanggung jawab atas unit proses atau unit grup proses. Unit proses ini dapat berupa unit lisensor atau unit non-lisensor. Ini juga akan mencakup pekerjaan *revamping CDU*.

8.1.4. PMT / PIT

Mengacu dokumen Manajemen Antarmuka untuk definisi dan masing-masing peran *PMT* dan *PIT*.

Kontraktor Os&Us, Kontraktor ISBL dan Kontraktor ICSS harus bertukar informasi desain, perhitungan dan gambar melalui *Interface Query (IQ)* dan rapat koordinasi pada waktu yang tepat agar dapat melaksanakan lingkup pekerjaan masing-masing.

their respective scope of work. The role of the PMT in coordination of the IQ is described in the Interface Management document.

8.1.5. Package Vendor

Package Vendor is responsible for a process or mechanical specific package. All the associated instruments and shipped loose items shall be provided by the package vendor. The ISBL and Os&Us Contractors will be responsible for the management of the packages residing within their respective areas.

9. RECOMMENDED PROTECTION LAYERS

This non-exhaustive list of recommended protection layers shall be addressed by the ICSS cybersecurity plan, and reviewed by the OWNER, along with the recommendation mentioned in previous sections, such as backups and others. If any part of the list is not applicable, then it should be mentioned in the review document(s).

9.1 System Hardening

9.1.1. Removal of Unnecessary Services and Programs.

Post-contract award, the Vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the control system.

Peran *PMT* dalam koordinasi *IQ* dijelaskan dalam dokumen Manajemen Antarmuka.

8.1.5. Vendor Paket

Vendor Paket bertanggung jawab atas suatu proses atau paket mekanikal khusus. Semua instrumen terkait dan barang yang dikirim secara terurai harus disediakan oleh vendor paket. Kontraktor *ISBL* dan *Os&Us* akan bertanggung jawab atas pengelolaan paket yang berada di wilayah masing-masing.

9. LAPISAN-LAPISAN PROTEKSI YANG DIREKOMENDASIKAN

Daftar lapisan proteksi yang direkomendasikan yang kurang lengkap harus dilengkapi pada perencanaan keamanan siber *ICSS* dan ditinjau ulang oleh PEMILIK bersama dengan rekomendasi terkait seperti pencadangan dan lainnya. Jika ada bagian dari daftar yang tidak dapat diimplementasikan maka harus disebutkan dalam dokumen.

9.1 Penguatan Sistem

9.1.1. Penghapusan Layanan dan Program yang Tidak Perlu.

Pasca-kontrak, Vendor harus menyediakan dokumen yang merinci semua aplikasi, utilitas, layanan sistem, skrip, file konfigurasi, database, dan semua perangkat lunak lain yang diperlukan dan konfigurasi yang sesuai, termasuk revisi dan/atau semua *patch* sistem komputer yang terkait dengan sistem kontrol.

The Vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.	Vendor harus menyediakan daftar layanan yang diperlukan untuk setiap sistem komputer yang menjalankan aplikasi sistem kontrol atau yang diperlukan untuk menghubungkan aplikasi sistem kontrol. Daftar tersebut harus mencakup semua *port* dan layanan yang diperlukan untuk operasi normal serta setiap *port* dan layanan lain yang diperlukan untuk operasi darurat. Daftar tersebut harus mencakup penjelasan atau referensi nya untuk menjelaskan mengapa setiap layanan diperlukan.
The Vendor shall verify and provide documentation that all services are patched to current status.	Vendor harus memverifikasi dan memberikan dokumentasi bahwa semua layanan sudah dilengkapi dengan *patch* status terakhir.
The Vendor shall provide appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.	Vendor harus menyediakan solusi pembaruan perangkat lunak dan layanan yang sesuai untuk mengurangi tingkat kerentanan produk dalam rangka mempertahankan tingkat keamanan sistem sesuai yang ditetapkan.
The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the control system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to: • Games. • Device drivers for network devices not delivered.	Vendor harus menghapus dan/atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan sistem kontrol sebelum *FAT. Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan. Perangkat lunak yang akan dihapus dan/atau dinonaktifkan harus mencakup, namun tidak terbatas pada: • Game • *Driver* dari seluruh komponen perangkat jaringan yang tidak terkirim.

• Messaging services (e.g. MSN, AOL IM).	• Layanan pesan (mis. *MSN, AOL IM).*
• Servers or clients for unused Internet services.	• *Server* atau Client dalam layanan Internet yang tidak digunakan.
• Software compilers in all user workstations and servers except for development workstations and servers.	• Kompiler perangkat lunak di semua *workstation* dan *server* pengguna kecuali *compiler* yang diperlukan untuk pengembangan *workstation* dan *server*.
• Software compilers for languages that are not used in the control system	• Kompiler perangkat lunak untuk bahasa pemograman yang tidak digunakan dalam sistem kontrol
• Unused networking and communications protocols.	• Protokol jaringan dan komunikasi yang tidak digunakan.
• Unused administrative utilities, diagnostics, network management, and system management functions.	• Utilitas administratif, diagnostik, manajemen jaringan, dan fungsi manajemen sistem yang tidak digunakan.
• Backups of files, databases, and programs used only during system development.	• Cadangan file, database, dan program yang hanya digunakan selama pengembangan sistem.
• All unused data and configuration files.	• Semua data dan file konfigurasi yang tidak digunakan.
• Sample programs and scripts.	• Contoh program dan skrip
• Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).	• Utilitas pemrosesan dokumen yang tidak digunakan *(Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, dll.).*
9.1.2. Host Intrusion Detection System (HIDS)	9.1.2. Sistem Deteksi Intrusi *Host*.
The Vendor shall provide a configured HIDS and/or provide the information to configure a HIDS to include, but not be limited to, static file names, dynamic file name patterns, system and user accounts, and execution of unauthorized code, host utilization, and process permissions sufficient for configuring	Vendor harus menyediakan konfigurasi *HIDS* dan/atau informasi untuk mengonfigurasi *HIDS*, dan tidak terbatas pada nama file statis, pola nama file dinamis, sistem dan akun pengguna, eksekusi kode yang tidak sah, pemanfaatan host, dan proses perizinan yang cukup untuk mengkonfigurasi *HIDS*.

the HIDS.	
The Vendor shall configure the HIDS such that all system and user account connections are logged. This log will be configured such that an alarm can be displayed to the operator or security personnel if an abnormal situation occurs and does not negatively impact the operating system functions or business objectives.	Vendor harus mengonfigurasi *HIDS* sedemikian rupa sehingga semua koneksi sistem dan akun pengguna dicatat. Log ini akan dikonfigurasi sedemikian rupa sehingga alarm dapat dibaca operator atau personel keamanan pada saat terjadi situasi yang tidak normal dan tidak berdampak negatif terhadap fungsi sistem operasi atau tujuan bisnis.
The Vendor shall recommend log review and notification software tools.	Vendor harus merekomendasikan tinjauan terhadap log dan notifikasi perangkat lunak.
The Vendor shall configure devices as “append only” to prevent alteration of records on local storage devices.	Vendor harus mengkonfigurasi perangkat sebagai "hanya tambahan” untuk mencegah terhadap perubahan catatan pada perangkat penyimpanan lokal.
9.1.3. Changes to File System and Operating System Permissions.	9.1.3. Perubahan perizinan Sistem File dan Sistem Operasi.
The Vendor shall configure hosts with least privilege file and account access and provide documentation of the configuration.	Vendor harus mengonfigurasi *host* dengan akses file dan akun yang paling sedikit dan menyediakan dokumentasi konfigurasi.
The Vendor shall configure the necessary system services to execute at the least user privilege level possible for that service and provide documentation of the configuration.	Vendor harus mengkonfigurasi layanan sistem yang diperlukan untuk menjalankan fungsi penyediaan layanan minimal pada tingkat hak istimewa pada pengguna dan untuk menyediakan konfigurasi dokumentasi
The Vendor shall document that changing or disabling access to such files and functions has been completed.	Vendor harus mendokumentasikan bahwa perubahan atau penonaktifan akses ke file dan fungsi tersebut telah selesai.
9.1.4. Hardware Configuration.	9.1.4. Konfigurasi Perangkat Keras
The Vendor shall disable, through software or physical disconnection, all unneeded communication ports and removable media drives, or	Vendor harus menonaktifkan, melalui perangkat lunak atau pemutusan secara fisik, semua port komunikasi yang tidak dibutuhkan dan

provide engineered barriers, and provide documentation of the results.	menyediakan drive media yang dapat dilepas, atau menyediakan rekayasa penghalangan, dan memberikan dokumentasi hasilnya.
The Vendor shall password protect the BIOS from unauthorized changes unless it is not technically feasible, in which case the Vendor shall document this case and provide mitigation measures.	Vendor harus melindungi *BIOS* dari perubahan yang dilakukan secara tidak sah dengan password kecuali secara teknis tidak memungkinkan, dalam hal ini Vendor harus mendokumentasikan kasus ini dan memberikan langkah-langkah mitigasi.
The Vendor shall provide a written list of all disabled or removed USB ports, CD/DVD drives, and other removable media devices.	Vendor harus memberikan daftar tertulis dari semua port USB yang dinonaktifkan atau dilepas, drive CD/DVD, dan perangkat media lepas lainnya.
The Vendor shall configure the network devices to limit access to/from specific locations, where appropriate, and provide documentation of the configuration.	Vendor harus mengkonfigurasi perangkat jaringan untuk membatasi akses ke/dari lokasi tertentu, jika sesuai, dan memberikan dokumentasi konfigurasi.
The Vendor shall configure the system to allow the system administrators the ability to re-enable devices if the devices are disabled by software and provide documentation of the configuration.	Vendor harus mengkonfigurasi sistem untuk memungkinkan administrator sistem mengaktifkan kembali perangkat jika perangkat dinonaktifkan oleh perangkat lunak dan memberikan dokumentasi konfigurasi.
9.1.5. Heartbeat Signals.	9.1.5. Sinyal *heartbeat*
The Vendor shall identify heartbeat signals or protocols and recommend whether any should be included in network monitoring.	Vendor harus mengidentifikasi sinyal atau protokol *heartbeat* dan merekomendasikan apakah ada yang harus disertakan dalam pemantauan jaringan.
Post-contract award, the Vendor shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic if the signals are included in the network monitoring.	Pasca-kontrak, Vendor harus memberikan definisi paket dari sinyal *heartbeat* dan contoh lalu lintas *heartbeat* jika sinyal tersebut sudah ada dalam pemantauan jaringan.

In designing the heartbeat signals, Vendor shall determine and set the time of communication timeout that shall not degrading the performance of ICSS.	Dalam mendesain sinyal heartbeat, Vendor harus menentukan dan mengatur waktu timeout komunikasi dimana dengan waktu *heartbeat* tersebut tidak akan menurunkan kinerja *ICSS*.
9.1.6. Installing Operating Systems, Applications, and Third-Party Software Updates.	9.1.6. Menginstal Sistem Operasi, Aplikasi, dan Pembaruan Perangkat Lunak Pihak Ketiga.
The Vendor shall have a patch management and update process.	Vendor harus memiliki manajemen *patch* dan proses pembaruan.
Pre-contract award, the Vendor shall provide details on their patch management and update process. Responsibility for installation and update of patches shall be identified.	Sebelum tahap kontrak, Vendor harus memberikan perincian tentang manajemen *patch* dan proses pembaruan mereka. Tanggung jawab instalasi dan pembaruan *patch* harus dijelaskan.
Post-contract award, the Vendor shall provide notification of known vulnerabilities affecting Vendor-supplied or required OS, application, and third-party software within 3 weeks after public disclosure.	Paska kontrak, Vendor harus menyediakan notifikasi tentang kerentanan yang mempengaruhi *OS*, aplikasi, dan perangkat lunak yang dipasok oleh pihak ketiga dalam waktu 3 minggu setelah hal tersebut diberitahukan ke publik.
Post-contract award, the Vendor shall provide notification of patches affecting security within 3 weeks as identified in the patch management process. The Vendor shall apply, test, and validate the appropriate updates and/or workarounds on a baseline reference system before distribution. Mitigation of these vulnerabilities shall occur within 3 weeks.	Paska kontrak, Vendor harus memberikan pemberitahuan tentang *patch* yang mempengaruhi keamanan dalam waktu 3 minggu seperti yang diidentifikasi dalam proses manajemen *patch*. *Vendor* harus menerapkan, menguji, dan memvalidasi pembaruan dan/atau solusi yang sesuai pada sistem referensi dasar sebelum didistribusikan. Mitigasi kerentanan ini akan terjadi dalam waktu 3 minggu.
9.1.7. Application Whitelisting.	9.1.7. Aplikasi *Whitelisting*
The Vendor shall have an application whitelisting system in place.	Vendor harus memiliki sistem aplikasi *Whitelisting*.

The Vendor shall provide the full list of allowable executables for each of the servers, workstation and embedded systems. The basis of the rule set for this list shall be “deny all,” with exceptions explicitly identified by the Vendor.	Vendor harus menyediakan daftar lengkap file yang dapat dieksekusi yang diizinkan untuk setiap *server, workstation*, dan sistem yang sudah ada didalamnya. Dasar aturan yang ditetapkan untuk daftar ini adalah “tolak semua”, dengan pengecualian yang secara eksplisit diidentifikasi oleh Vendor.
This information is deemed business sensitive and shall be protected as such.	Informasi ini dianggap hal yang sensitif dan harus dilindungi.
9.2 Perimeter Protection	9.2 Proteksi *Perimeter*
9.2.1. Firewalls.	*9.2.1. Firewalls*
The Vendor shall provide firewalls and firewall rule sets between network zones or provide firewall rule sets if the firewalls are not provided by the Vendor.	Vendor harus menyediakan *firewall* dan prosedur pengaturan *firewall* antar zona jaringan atau hanya menyediakan prosedur pengaturan *firewall* jika *firewall* tidak disediakan oleh Vendor.
The Vendor shall provide firewall rule sets and/or other equivalent documentation. The basis of the rule set shall be “deny all,” with exceptions explicitly identified by the Vendor.	Vendor harus menyediakan sejumlah prosedur pengaturan *firewall* dan/atau dokumentasi. Dasar dari aturan yang ditetapkan adalah “tolak semua”, dengan pengecualian yang secara eksplisit diidentifikasi oleh Vendor.
This information is deemed business sensitive and shall be protected as such.	Informasi ini dianggap hal yang sensitif dan harus dilindungi seperti itu.
Post-contract award, the Vendor shall provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding rule sets.	Paska kontrak,Vendor harus memberikan informasi terperinci tentang semua komunikasi (termasuk protokol) yang diperlukan melalui *firewall*, baik *inbound* atau *outbound*, dan mengidentifikasi setiap perangkat jaringan yang memulai komunikasi sesuai dengan prosedur pengaturan terkait.
9.2.2. Network Intrusion Detection System (NIDS)	9.2.2. Sistem Deteksi Intrusi Jaringan

	Pre-contract award, the Vendor shall provide a recommended placement of the NIDS within the control system network.	Penghargaan pra-kontrak, Vendor harus menyediakan rekomendasi terhadap penempatan *NIDS* dalam jaringan sistem kontrol.
	The Vendor shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries, for anomaly-based NIDSs.	Vendor harus menyediakan profil lalu lintas dengan jalur komunikasi yang diharapkan, lalu lintas jaringan, dan batas pemanfaatan yang diharapkan, untuk *NIDS* juga harus disediakan profil lalu lintas yang berbasis anomali.
	The Vendor shall provide appropriate signatures, for signature-based NIDSs.	Vendor harus memberikan tanda tangan yang sesuai, pada *NIDS* berbasis tanda tangan
	Post-contract award, the Vendor shall provide a configured NIDS and/or provide the information to configure a NIDS.	Paska kontrak, Vendor harus melakukan konfigurasi *NIDS* dan/atau memberikan informasi untuk mengonfigurasi *NIDS*.
9.2.3.	Honey pots / Canaries.	*9.2.3. Honey pots / Canaries*
	Honey pots (which analyze unauthorized connections) and/or Canary(ies) (which flag that a connection attempt has taken place) have been implemented in certain network configurations to provide passive network monitoring.	*Honey pot* (yang menganalisis suatu koneksi yang tidak sah) dan/atau *Canary* (yang menandai bahwa upaya koneksi telah dilakukan) telah diterapkan dalam konfigurasi jaringan tertentu untuk menyediakan pemantauan jaringan pasif.
	Pre-contract award, the Vendor shall provide a recommended placement of the canary(ies) within the control system network.	Sebelum tahap kontrak Vendor harus memberikan rekomendasi terhadap penempatan dari *Canary* dalam jaringan sistem kontrol.
	The canary(ies) shall be configured with alerting software to indicate unauthorized connection attempts.	*Canary* harus dikonfigurasi dengan perangkat lunak yang dapat otomatis memberikan peringatan yang menunjukkan adanya koneksi yang tidak sah.
	Post-contract award, the Vendor shall provide a configured canary(ies) or information to configure a canary(ies).	Paska kontrak, Vendor harus mengkonfigurasi *canary* atau memberikan prosedur konfigurasi canary.
9.2.4.	IP Obfuscation.	9.2.4. Penyembunyian *IP*

IP obfuscation (IPO) is made of devices that communicate between themselves without using IP and obfuscate (hide) the IP address of the devices under their protection, without impeding the functioning of the system as a whole.

Pre-contract award, the Vendor shall provide a recommended placement of the IPO devices within the control system network.

The IPO devices shall be configured to allow proper segregation of devices that require communication, in parallel to the implemented IP segregation.

Post-contract award, the Vendor shall provide a complete map of the IPO devices and their configuration.

Penyembunyian *IP (IPO)* dibuat dari perangkat yang berkomunikasi di antara mereka sendiri tanpa menggunakan IP dan mengaburkan (menyembunyikan) alamat IP perangkat di bawah proteksinya, tanpa menghalangi fungsi sistem secara keseluruhan.

Sebelum tahap kontrak Vendor harus memberikan rekomendasi penempatan perangkat *IPO* dalam jaringan sistem kontrol.

Perangkat IPO harus dikonfigurasi untuk memungkinkan pemisahan perangkat yang membutuhkan komunikasi secara paralel dengan pemisahan *IP* yang diterapkan.

Paska kontrak, Vendor harus menyediakan peta lengkap perangkat *IPO* dan konfigurasinya.

9.3 Account Management

9.3.1. Disabling, Removing, or Modifying Well-Known or Guest Accounts.

Disabling, removing, or modifying well-known or guest accounts and changing default passwords are necessary to reduce system vulnerabilities.

9.3.2. Session Management.

The Vendor shall not permit user credentials to be transmitted in clear text.

The Vendor shall provide the strongest encryption method commensurate with the technology platform and response time constraints.

The Vendor shall not allow multiple concurrent logins, applications to

9.3 Manajemen Akun

9.3.1. Menonaktifkan, Menghapus, atau Memodifikasi Akun yang dikenal atau Akun Tamu.

Menonaktifkan, menghapus, atau memodifikasi akun yang dikenal atau akun tamu dan mengubah kata sandi bawaan yang diperlukan untuk mengurangi kerentanan sistem.

9.3.2. Manajemen sesi.

Vendor tidak akan mengizinkan kredensial pengguna untuk dikirim dalam bentuk teks asli.

Vendor harus menyediakan metode enkripsi terkuat yang sepadan dengan platform teknologi dan batasan waktu respons

Vendor tidak boleh mengizinkan beberapa login yang bersamaan,

retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

The Vendor shall provide user account-based logout and timeout settings.

9.3.3. Password/Authentication Policy and Management.

The Vendor shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password.

The Vendor shall not store passwords electronically or in Vendor-supplied hardcopy documentation in clear text unless the media is physically protected.

The Vendor shall control configuration interface access to the account management system.

The Vendor shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations, where system availability would be negatively impacted by normal security procedures.

9.3.4. Account Auditing and Logging.

The Vendor shall provide a system whereby account activity is logged

aplikasi untuk menyimpan informasi login di antara sesi, menyediakan fungsionalitas pengisian otomatis selama *login*, atau mengizinkan *login* anonim.

Vendor harus menyediakan pengaturan *logout* dan batas waktu pada akun pengguna.

9.3.3. Kebijakan dan Manajemen Kata Sandi/Otentikasi.

Vendor harus menyediakan sistem manajemen kata sandi akun yang dapat dikonfigurasi yang memungkinkan pemilihan panjang kata sandi, frekuensi perubahan, pengaturan kompleksitas kata sandi yang diperlukan, jumlah upaya masuk, keluar sesi tidak aktif, kunci layar oleh aplikasi, dan penolakan penggunaan berulang atau daur ulang sandi yang sama.

Vendor tidak boleh menyimpan kata sandi secara elektronik atau dalam dokumentasi hardcopy yang disediakan Vendor dalam bentuk teks asli kecuali media tersebut dilindungi secara fisik.

Vendor harus mengontrol akses antarmuka konfigurasi ke sistem manajemen akun.

Vendor harus menyediakan mekanisme untuk mengembalikan kebijakan otentikasi keamanan selama pemulihan sistem darurat atau operasi abnormal lainnya, di mana ketersediaan sistem akan terpengaruh secara negatif oleh prosedur keamanan normal.

9.3.4. Audit dan Pencatatan Akun.

Vendor harus menyediakan sistem dimana aktivitas akun dicatat dan

	and is auditable both from a management (policy) and operational (account use activity) perspective.	dapat diaudit baik dari perspektif manajemen (kebijakan) dan operasional (aktivitas penggunaan akun).
	The Vendor shall time stamp, encrypt, and control access to audit trails and log files.	Vendor harus melakukan time stamp, enkripsi, dan kontrol akses ke jejak audit dan log file.
	The Vendor shall ensure audit logging does not adversely impact system performance requirements. The Vendor shall provide read-only media for log creation.	Vendor harus memastikan bahwa pencatatan audit tidak berdampak buruk pada persyaratan kinerja sistem. Vendor harus menyediakan media *read-only* untuk pembuatan *log*.
9.3.5.	Role-Based Access Control for Control System Applications.	9.3.5. Kontrol Akses Berbasis Peran untuk Aplikasi Sistem Kontrol.
	The Vendor shall provide for user accounts with configurable access and permissions associated with the defined user role.	Vendor harus menyediakan akun pengguna dengan akses dan izin yang dapat dikonfigurasi terkait dengan peran pengguna yang ditentukan.
	The Vendor shall adhere to least privileged permission schemes for all user accounts, and application-to-application communications.	Vendor harus mematuhi skema perizinan dengan hak istimewa terendah untuk semua akun pengguna, dan komunikasi dari aplikasi-ke-aplikasi.
	The Vendor shall configure the system so that initiated communications start with the most privileged application controlling the communication. Upon failed communication, the most privileged side will restart communications.	Vendor harus mengkonfigurasi sistem sehingga komunikasi yang dimulai dengan aplikasi paling istimewa yang mengendalikan komunikasi. Setelah komunikasi gagal, pihak yang paling diistimewakan akan memulai kembali komunikasi.
	The Vendor shall verify that the master network device initiates communications.	Vendor harus memverifikasi bahwa perangkat jaringan master mengawali komunikasi.
	The Vendor shall inform the Purchaser if this condition cannot be met.	Vendor harus menginformasikan Pembeli jika kondisi ini tidak dapat dipenuhi.
	The Vendor shall verify that a user cannot escalate privileges, under	Vendor harus memverifikasi bahwa pengguna tidak dapat merubah hak

any circumstances, without logging into a higher-privileged role first.	keistimewaannya, dalam keadaan apa pun, tanpa masuk ke peran hak keistimewaan yang lebih tinggi terlebih dahulu.
The Vendor shall provide a mechanism for changing user(s) role (e.g. group) associations.	Vendor harus menyediakan mekanisme untuk mengubah asosiasi peran pengguna (misalnya grup).
Post-contract award, the Vendor shall provide documentation defining access and security permissions, user accounts, applications, and communication paths with associated roles.	Paska kontrak,Vendor harus menyediakan dokumentasi yang menentukan akses dan perizinan keamanan, akun pengguna, aplikasi, dan jalur komunikasi dengan peran terkait
9.3.6. Single Sign-On (SSO).	9.3.6. Sistem Masuk Tunggal.
The Vendor shall provide an SSO such that role-based access control (RBAC) enforcement is equivalent to that enforced as a result of direct login.	Vendor harus menyediakan *SSO* sedemikian rupa sehingga penegakan kontrol akses berbasis peran *(RBAC)* setara dengan yang diberlakukan sebagai hasil dari *login* langsung.
The Vendor shall provide a means of allowing SSO to a suite of applications via secure shell (SSH), terminal services, or other authenticated means. This system shall be RBAC capable.	Vendor harus menyediakan sarana yang memungkinkan *SSO* ke rangkaian aplikasi melalui *SSH*, layanan terminal, atau sarana terotentikasi lainnya. Sistem ini harus mampu *RBAC*.
The Vendor shall provide documentation on configuring such a system, and documentation showing equivalent results in running validation tests against the direct login and the SSO.	*Vendor* harus memberikan dokumentasi tentang konfigurasi sistem tersebut, dan dokumentasi yang menunjukkan hasil yang setara dalam menjalankan uji validasi terhadap login langsung dan *SSO*.
The Vendor shall protect key files and access control lists (ACLs) used by the SSO system from non-administrative user read, write, and delete access. The SSO must resolve individual user's logins to each application.	Vendor harus melindungi file kunci dan daftar kontrol akses (*ACL*) yang digunakan oleh sistem *SSO* dari akses baca, tulis, dan hapus pengguna non-administratif. *SSO* harus menyelesaikan login pengguna individu ke setiap aplikasi.
9.4 Malware Detection And Protection	9.4 Deteksi Dan Proteksi Perangkat Lunak

Malware Detection and Protection

Malware is any unauthorized software. Because many control networks are connected to other networks or updated by media, malware can enter into the network and affect process control and/or communications. Malware consists of many different types of software and may include, but is not limited to, bots, Trojans, worms, viruses, backdoors, and zombies. Malware detection can occur on a host or a network-based device.

Updates to malware detection software may adversely impact control system behavior.

The Vendor shall disclose the existence and reasons for any known or identified backdoor codes. The Vendor shall meet one of two conditions:

- Provide a host-based malware detection scheme for the control system network. The Vendor shall verify adequate system performance for host-based malware detection, quarantine (instead of automatically deleting) suspected infected files, and provide an updating scheme for the signatures. The Vendor shall also test major updates to malware detection applications and provide performance measurement data on the impact of using the malware detection applications in an active system. Measurements shall include, but are not limited to network usage, CPU usage, memory usage, and any other impact to normal communications processing.

9.4.1. Deteksi dan Proteksi *Malware*.

Malware adalah perangkat lunak yang tidak sah. Karena banyak jaringan kontrol terhubung ke jaringan lain atau diperbarui oleh media, *malware* dapat masuk ke jaringan dan memengaruhi kontrol proses dan/atau komunikasi. *Malware* terdiri dari berbagai jenis perangkat lunak dan mungkin termasuk, namun tidak terbatas pada, *bot, Trojan, worm, virus, backdoor, dan zombie*. Deteksi *malware* dapat terjadi pada *host* atau perangkat berbasis jaringan.

Pembaruan perangkat lunak pendeteksi malware dapat berdampak buruk pada perilaku sistem kontrol.

Vendor harus mengungkapkan keberadaan dan alasan untuk setiap kode *backdoor* yang diketahui atau diidentifikasi. Vendor harus memenuhi salah satu dari dua kondisi:

- Menyediakan skema deteksi malware berbasis *host* untuk jaringan sistem kontrol. *Vendor* harus memverifikasi kinerja sistem yang memadai untuk deteksi *malware* berbasis *host*, karantina (bukan menghapus secara otomatis) file yang dicurigai terinfeksi, dan menyediakan skema pembaruan untuk tanda tangan. Vendor juga harus menguji pembaruan besar untuk aplikasi pendeteksi malware dan memberikan data pengukuran kinerja tentang dampak penggunaan aplikasi pendeteksi malware dalam sistem yang aktif. Pengukuran harus mencakup, namun tidak terbatas pada penggunaan jaringan, penggunaan *CPU*, penggunaan memori, dan dampak lain apa pun terhadap pemrosesan

- If the Vendor is not providing the actual host-based malware detection scheme, the Vendor shall suggest malware detection products to be used and provide guidance on malware detection settings that will work with Vendor products.

9.5 Host Name Resolution

9.5.1. Network Addressing and Name Resolution.

Pre-contract award, the Vendor shall provide recommended network addressing and name resolution methodology.

The Vendor shall provide a means to verify the integrity of configuration files, zone data, and other DNS files (e.g. such integrity checking may be done with a HIDS).

Post-contract award, the Vendor shall provide a configured DNS server(s) or the information to configure a DNS server(s) that meets stringent standards of security for ICSS.

The Vendor shall consider addressing information as business sensitive (Level 1 - Strictly Confidential) and protect it as such.

9.6 End Device

9.6.1. Intellegent Electronic Devices

An intelligent electronic device (IED) is sometimes referred to as an intelligent end device. It incorporates microprocessors within the device, receives information from process

komunikasi normal.

- Jika *Vendor* tidak menyediakan skema deteksi *malware* berbasis *host* yang sebenarnya, *Vendor* harus membuat rekomendasi tentang produk deteksi *malware* yang digunakan dan memberikan panduan tentang pengaturan deteksi *malware* yang akan bekerja dengan produk *Vendor*.

9.5 Resolusi Nama *Host*

9.5.1. Pengalamatan Jaringan dan Resolusi Nama

Sebelum tahap kontrak, Vendor harus memberikan pengalamatan jaringan yang direkomendasikan dan metodologi resolusi nama.

Vendor harus menyediakan sarana untuk memverifikasi integritas file konfigurasi, data zona, dan file *DNS* lainnya (misalnya, pemeriksaan integritas tersebut dapat dilakukan dengan *HIDS*).

Paska kontrak, Vendor harus menyediakan server DNS yang dikonfigurasi atau informasi untuk mengkonfigurasi server DNS yang memenuhi standar keamanan yang ketat dari ICSS.

Vendor harus mempertimbangkan untuk menangani informasi sebagai hal yang sensitif (Level 1 - Sangat Rahasia) dan memberikan proteksi seperti itu.

9.6 Perangkat Akhir

9.7.1. Perangkat Elektronik Cerdas

Perangkat elektronik cerdas (*IED)* kadang-kadang disebut sebagai perangkat akhir yang cerdas. Ini menggabungkan mikroprosesor di dalam perangkat, menerima

sensors or from the power equipment, and issues control commands to process equipment such as breakers, valves, pumps, transformers, etc.	informasi dari sensor proses atau dari peralatan listrik, dan mengeluarkan perintah kontrol untuk memproses peralatan seperti pemutus, valve, pompa, transformator, dll.
The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.	Vendor harus menyediakan fitur keamanan fisik dan cyber, termasuk namun tidak terbatas pada otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan komputer konfigurasi dari modifikasi atau penggunaan yang tidak sah.
The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.	Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan cyber dan menyediakan metodologi untuk memelihara fitur termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi Vendor atau manufaktur.
The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.	Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, bandwidth, waktu respons, dan throughput, termasuk selama SAT yang terhubung ke peralatan yang ada.
The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.	Vendor harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*. *Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.
The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to	Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang

maintain the established level of system security.

The Vendor shall verify and provide documentation that the safety instrumented system (SIS) is certified after incorporating the security devices.

9.6.2. Remote Terminal Units.

A remote terminal unit (RTU) is a microprocessor-controlled device that is used to provide system control of industrial processes.

The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and

terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.

Vendor harus memverifikasi dan memberikan dokumentasi yang menyatakan bahwa Sistem Instrumentasi Safety (SIS) baru dapat disertifikasi setelah memasukkan perangkat keamanannya.

9.7.2. Unit Terminal Jarak Jauh

Unit terminal jarak jauh (*RTU)* adalah perangkat yang dikendalikan mikroprosesor yang digunakan untuk menyediakan sistem kontrol proses industri.

Vendor harus menyediakan fitur keamanan fisik dan siber termasuk namun tidak terbatas pada otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan konfigurasi komputer dari modifikasi atau penggunaan yang tidak sah.

Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi pemeliharaan fitur, termasuk metode untuk mengubah pengaturan kondisi *default* yang dibuat oleh Vendor atau manufaktur.

Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama *SAT* yang terhubung ke peralatan yang ada.

Vendor harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan

maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*. Vendor harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.

The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

Vendor harus memverifikasi dan memberikan dokumentasi bahwa SIS disertifikasi setelah memasukkan perangkat keamanan.

9.6.3. Programmable Logic Controllers.

9.7.3. Pengontrol Logika yang dapat diprogram.

The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Vendor harus menyediakan fitur keamanan fisik dan siber termasuk namun tidak terbatas pada otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan konfigurasi komputer dari modifikasi atau penggunaan yang tidak sah.

The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi untuk memelihara fitur, termasuk metode untuk mengubah pengaturan dari kondisi *default* yang dikonfigurasi *Vendor* atau manufaktur.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing

Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama *SAT* saat terhubung ke peralatan

equipment.	yang ada.
The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.	Vendor harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*. *Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.
The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.	Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.
The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices	Vendor harus memverifikasi dan memberikan dokumentasi yang menyatakan bahwa *SIS* disertifikasi setelah memasukkan perangkat keamanan
9.6.4. Sensors, Actuators, and Meters.	9.7.4. Sensor, Aktuator, dan Meter.
The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.	Vendor harus menyediakan fitur keamanan fisik dan siber termasuk, namun tidak terbatas pada, otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan komputer konfigurasi dari modifikasi atau penggunaan yang tidak sah.
The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.	Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi untuk memelihara fitur, termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall provide secure	*Vendor* harus menyediakan jalur

(serial, Ethernet, and wireless) communication paths, including the ability to filter and monitor communications.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment. For smart devices:

- The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

- The Vendor shall provide, within a pre-negotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

- The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

9.7 Remote Access

9.7.1. Dial-Up Modems.

The Vendor shall verify that modems are enabled only when needed (e.g. time constraint) or limit possible entry points (e.g. access list).

komunikasi yang aman (serial, *Ethernet,* dan nirkabel), termasuk kemampuan untuk menyaring dan memantau komunikasi.

Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama *SAT* saat terhubung ke peralatan yang ada. Untuk perangkat pintar:

- Vendor harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum FAT. Vendor harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.

- Vendor harus menyediakan pembaruan dan/atau solusi perangkat lunak dan layanan yang sesuai untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan dalam periode pra-negosiasi.

- Vendor harus memverifikasi dan memberikan dokumentasi yang menyatakan bahwa SIS disertifikasi setelah memasukkan perangkat keamanan.

9.7 Akses Jarak Jauh

9.7.1. *Modem Dial-Up*.

Vendor harus memverifikasi bahwa modem diaktifkan hanya bila diperlukan (misalnya dengan batasan waktu) atau membatasi kemungkinan

	titik masuk (misalnya daftar akses).
The Vendor shall change or disable configuration settings that could be used for exploitation when not needed.	*Vendor* harus mengubah atau menonaktifkan pengaturan konfigurasi yang dapat digunakan untuk dapat digunakan untuk eksploitasi bila tidak diperlukan.
The Vendor shall provide a telephony firewall to include authorized list, automatic block, and alarm during unauthorized access and automatic log review.	*Vendor* harus menyediakan *firewall* untuk sistem telepon yang menyertakan daftar resmi, pemblokiran otomatis, dan alarm selama akses tidak sah dan tinjauan log otomatis.
The Vendor shall not permit user credentials to be transmitted in clear text.	*Vendor* tidak akan mengizinkan kredensial pengguna untuk dikirim dalam bentuk teks asli.
The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.	*Vendor* harus menyediakan fitur keamanan fisik dan siber termasuk namun tidak terbatas pada otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan konfigurasi komputer dari modifikasi atau penggunaan yang tidak sah.
The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.	*Vendor* harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi untuk memelihara fitur, termasuk metode untuk mengubah pengaturan dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.	*Vendor* harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth,* waktu respons, dan throughput, termasuk selama *SAT* saat terhubung ke peralatan yang ada.
The Vendor shall provide a list including all ports and services	*Vendor* harus memberikan daftar termasuk semua *port* dan layanan

required for normal operation and emergency operation and troubleshooting.

The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the modem and modem security system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but is not limited to:

- Device drivers for network devices not delivered.
- Unused networking and communications protocols.
- Unused administrative utilities, diagnostics, network management, and system management functions.
- All unused data and configuration files.

The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product.

yang diperlukan untuk operasi normal dan operasi darurat dan pemecahan masalah.

Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.

Vendor harus menghapus dan/atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan modem dan sistem keamanan modem sebelum *FAT. Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan. Perangkat lunak yang akan dihapus dan/atau dinonaktifkan harus mencakup, namun tidak terbatas pada:

- *Driver* untuk perangkat jaringan yang tidak terkirim.
- Jaringan dan protokol komunikasi yang tidak digunakan.
- Utilitas administratif, diagnostik, manajemen jaringan, dan fungsi manajemen sistem yang tidak digunakan.
- Semua data dan file konfigurasi yang tidak digunakan.

Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

Post-contract award, the Vendor shall provide documentation detailing all modem configurations, services, and all software/modem device protection configurations and keys, including revisions and/or patch levels.

9.7.2. Dedicated Line Modems.

The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall not permit user credentials to be transmitted in clear text.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall provide a list

Vendor harus memverifikasi dan memberikan dokumentasi yang menyatakan bahwa *SIS* disertifikasi setelah memasukkan perangkat keamanan.

Paska kontrak, Vendor harus memberikan dokumentasi yang merinci semua konfigurasi modem, layanan, dan semua konfigurasi dan kunci proteksi perangkat lunak/perangkat modem, termasuk revisi dan/atau tingkat patch.

9.7.2. Modem Jalur Khusus.

Vendor harus menyediakan fitur keamanan fisik dan cyber termasuk, namun tidak terbatas pada, otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan komputer konfigurasi dari modifikasi atau penggunaan yang tidak sah.

Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan cyber dan menyediakan metodologi untuk memelihara fitur termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi Vendor atau manufaktur.

Vendor tidak boleh mengizinkan kredensial pengguna untuk dikirim dalam teks yang jelas.

Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama *SAT* saat terhubung ke peralatan yang ada.

Vendor harus memberikan daftar

including all ports and services required for normal operation and emergency operation and troubleshooting.

The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the modem and modem security system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but not be limited to:

- Device drivers for network devices not delivered.
- Unused networking and communications protocols.
- Unused administrative utilities, diagnostics, network management, and system management functions.
- All unused data and configuration files.

Post-contract award, the Vendor shall provide documentation detailing all modem configurations, services, and all software/modem device protection configurations and

semua *port* dan layanan yang diperlukan untuk operasi normal dan operasi darurat dan pemecahan masalah.

Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.

Vendor harus menghapus dan/atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan *modem* dan sistem keamanan *modem* sebelum *FAT*. *Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan. Perangkat lunak yang akan dihapus dan/atau dinonaktifkan harus mencakup, namun tidak terbatas pada:

- Driver perangkat untuk perangkat jaringan yang tidak terkirim.
- Protokol jaringan dan komunikasi yang tidak digunakan.
- Utilitas administratif, diagnostik, manajemen jaringan, dan fungsi manajemen sistem yang tidak digunakan.
- Semua data dan file konfigurasi yang tidak digunakan.

Paska kontrak, Vendor harus memberikan dokumentasi yang merinci semua konfigurasi modem, layanan, dan semua konfigurasi dan kunci proteksi perangkat

keys, including revisions and/or patch levels.

9.7.3. TCP/IP.

The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a pre-negotiated period, appropriate protocol stack updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the

lunak/perangkat modem, termasuk revisi dan/atau tingkat *patch*

9.7.3. TCP/IP

Vendor harus menyediakan fitur keamanan fisik dan siber termasuk namun tidak terbatas pada otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi perangkat dan komputer konfigurasi dari modifikasi atau penggunaan yang tidak sah.

Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi untuk memelihara fitur termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi Vendor atau manufaktur.

Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama SAT saat terhubung ke peralatan yang ada.

Vendor harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT. Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.

Vendor harus menyediakan, dalam periode pra-negosiasi, pembaruan beberapa protokol dan/atau solusi yang sesuai untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan

established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

The Vendor shall use a TCP/IP implementation that fully complies with the current TCP/IP request for comments (RFCs). The Vendor shall deliver a product that is IPv6 compatible.

The Vendor shall provide the ability to monitor traffic in an encryption scheme.

The Vendor shall provide, within 3 weeks, upgrades and patches to the protocol stack as vulnerabilities are identified to maintain the established level of system security.

Post-contract award, the Vendor shall provide an independent third-party security validation of the IPv6 implementations (e.g. using fuzzing techniques).

Post-contract award, the Vendor shall mitigate all vulnerabilities discovered during the testing of the IPv6 implementations and provide documentation of the results.

9.7.4. Web-based Interfaces.

The Vendor shall provide physical and cybersecurity features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features

sistem yang ditetapkan.

Vendor harus memverifikasi dan memberikan dokumentasi bahwa *SIS* disertifikasi setelah memasukkan perangkat keamanan.

Vendor harus menggunakan implementasi *TCP/IP* yang sepenuhnya sesuai dengan *RFC TCP/IP* saat ini. Vendor akan mengirimkan produk yang kompatibel dengan *IPv6*.

Vendor harus menyediakan kemampuan untuk memantau lalu lintas dalam skema enkripsi.

Vendor harus menyediakan, dalam waktu 3 minggu, pemutakhiran dan tambalan ke beberapa protokol saat kerentanan diidentifikasi untuk mempertahankan tingkat keamanan sistem yang ditetapkan.

Paska kontrak, Vendor harus menyediakan validasi keamanan pihak ketiga yang independen dari implementasi *IPv6* (misalnya menggunakan teknik *fuzzing*).

Paska kontrak, Vendor harus mengurangi semua kerentanan yang ditemukan selama pengujian implementasi IPv6 dan memberikan dokumentasi hasilnya.

9.7.4. Antarmuka berbasis *web*.

Vendor harus menyediakan fitur fisik dan keamanan siber termasuk, namun tidak terbatas pada, otentikasi, enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi sistem dari modifikasi atau penggunaan yang tidak sah.

Vendor harus secara jelas mengidentifikasi fitur keamanan fisik

and provide the methodologies for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.	dan siber dan menyediakan metodologi untuk memelihara fitur termasuk metode untuk mengubah pengaturan dari kondisi *default* yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.	Vendor harus memverifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama *SAT* saat terhubung ke peralatan yang ada.
The Vendor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run an HTTP server prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.	*Vendor* harus menghapus atau menonaktifkan semua komponen dan layanan perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat yang menjalankan *server HTTP* sebelum *FAT*. Vendor harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.
The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.	Vendor harus menyediakan, dalam waktu 3 minggu, pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.
The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.	Vendor harus memverifikasi dan memberikan dokumentasi bahwa *SIS* disertifikasi setelah memasukkan perangkat keamanan.
The Vendor shall provide documentation of input sanitization for all Web-form inputs including, but not limited to, measures for prevention of command injection, SQL injection, directory traversal, RFI, XSS, and buffer overflow.	Vendor harus menyediakan dokumentasi sanitasi input untuk semua input formulir *Web* termasuk namun tidak terbatas pada tindakan pencegahan injeksi perintah, injeksi *SQL,* direktori *traversal, RFI, XSS,* dan *buffer overflow.*

	The Vendor shall follow secure coding practices and reporting for all Web-based interface software. This requirement includes both Web applications and Web servers.	*Vendor* harus mengikuti praktik pengkodean yang aman dan pelaporan untuk semua perangkat lunak antarmuka berbasis *Web*. Persyaratan ini mencakup aplikasi *Web* dan *server Web.*
	The Vendor shall provide user configurable and managed passwords.	Vendor harus memberikan kata sandi yang dapat dikonfigurasi dan dikelola pengguna.
	The Vendor shall provide an independent third-party security code validation of all Web-based interface software.	Vendor harus menyediakan validasi kode keamanan pihak ketiga yang independen dari semua perangkat lunak antarmuka berbasis *Web.*
9.7.5.	Virtual Private Networks.	9.7.5. Jaringan Pribadi Virtual.
	The Vendor shall provide physical and cyber security features including, but not limited to, multifactor authentication (e.g. security token, known key, and/or certificate), encryption, access control, event and communication logging, monitoring, and alarming to protect the system and configuration computer from unauthorized modification or use.	Vendor harus menyediakan fitur keamanan fisik dan siber, termasuk namun tidak terbatas pada, otentikasi multifaktor (misalnya token keamanan, kunci yang diketahui, dan/atau sertifikat), enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi sistem dan konfigurasi komputer dari modifikasi atau penggunaan yang tidak sah.
	The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.	Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan metodologi untuk memelihara fitur, termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi Vendor atau manufaktur.
	The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.	Vendor harus melakukan verifikasi bahwa penambahan fitur keamanan tidak berdampak buruk pada konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput*, termasuk selama SAT saat terhubung ke peralatan yang ada.
	The Vendor shall remove or disable	Vendor harus menghapus atau

	all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.	menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT. Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.
	The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.	Vendor dalam waktu 3 minggu harus menyediakan pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.
	The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa SIS disertifikasi setelah memasukkan perangkat keamanan.
	The Vendor shall provide a DMZ outside the control network for the VPN server to reside.	Vendor harus menyediakan *DMZ* di luar jaringan kontrol agar *server VPN* berada.
	The Vendor shall use different authentication methods for establishing control network access and VPN connection.	Vendor harus menggunakan metode otentikasi yang berbeda untuk menetapkan akses jaringan kontrol dan koneksi *VPN*.
9.7.6.	Serial Communications Security.	9.7.6. Jaringan Pribadi Virtual.
	The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the serial communications and communication devices from unauthorized modification or use.	Vendor harus menyediakan fitur keamanan fisik dan siber, termasuk namun tidak terbatas pada, otentikasi multifaktor (misalnya token keamanan, kunci yang diketahui, dan/atau sertifikat), enkripsi, kontrol akses, pencatatan peristiwa dan komunikasi, pemantauan, dan alarm untuk melindungi sistem dan konfigurasi komputer dari modifikasi atau penggunaan yang tidak sah.
	The Vendor shall clearly identify the physical and cyber security features and provide the methodologies for	Vendor harus secara jelas mengidentifikasi fitur keamanan fisik dan siber dan menyediakan

maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.	metodologi untuk memelihara fitur, termasuk metode untuk mengubah pengaturan dari kondisi default yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall verify through security scans of the field communications that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified for serial communications, including during the SAT when connected to existing equipment.	*Vendor* harus melakukan verifikasi melalui pemindaian keamanan komunikasi lapangan bahwa penambahan fitur keamanan tidak mempengaruhi konektivitas, latensi, *bandwidth*, waktu respons, dan *throughput* yang ditentukan untuk komunikasi serial, termasuk selama *SAT* saat terhubung ke peralatan yang ada.
The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.	*Vendor* harus menghapus atau menonaktifkan semua komponen perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT. Vendor* harus memberikan dokumentasi tentang apa yang dihapus dan/atau dinonaktifkan.
The Vendor shall provide, within 3 weeks, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.	Vendor dalam waktu 3 minggu harus menyediakan pembaruan perangkat lunak dan layanan yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan produk dan untuk mempertahankan tingkat keamanan sistem yang ditetapkan.
The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa *SIS* disertifikasi setelah memasukkan perangkat keamanan.
9.8 Physical Security	9.8 Keamanan Fisik
9.8.1. Physical Access of Cyber Components	9.8.1. Akses Fisik Komponen Siber
The Vendor shall provide a detailed plan for appropriate physical security mechanisms.	Vendor harus memberikan rencana rinci untuk mekanisme keamanan fisik yang sesuai.

	The Vendor shall provide lockable or locking enclosures for control system components (e.g. servers, clients, and networking hardware).	Vendor harus menyediakan penutup yang dapat dikunci atau fasilitas penguncian untuk komponen sistem kontrol (misalnya *server*, klien, dan perangkat keras jaringan).
	The Vendor shall provide locking devices with a minimum of two keys per lock identifiable to each lock, and keyed or not keyed alike depending on Purchaser requirements.	Vendor harus menyediakan perangkat pengunci dengan minimal dua kunci per peralatan lengkap dengan fasilitas untuk dapat mengidentifikasi setiap kunci, fasilitas penguncian ini harus dapat memberikan fasilitas untuk dikunci atau tidak dikunci tergantung pada persyaratan Pembeli.
	The Vendor shall recommend a room locking device(s) where the equipment and workstations are located, if not already installed by the Purchaser.	Vendor harus merekomendasikan perangkat pengunci ruangan di mana peralatan dan workstation berada, jika belum dipasang oleh Pembeli.
	The Vendor shall verify and provide documentation that unauthorized logging devices are not installed (e.g. key loggers, cameras, and microphones).	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa perangkat *logging* yang tidak sah tidak dipasang (misalnya *key logger*, kamera, dan mikrofon).
	The Vendor shall provide two-factor authentication for physical access control.	*Vendor* harus menyediakan otentikasi dua faktor untuk kontrol akses fisik.
9.8.2.	Physical Perimeter Access.	9.8.2. Akses *Perimeter* Fisik.
	The Vendor shall provide a site security assessment, making special note of parameters or events that may influence physical intrusions. The results of this assessment shall be a documented site physical security plan.	*Vendo*r harus memberikan penilaian keamanan lokasi, membuat catatan khusus tentang parameter atau kejadian yang dapat mempengaruhi gangguan fisik. Hasil penilaian ini harus berupa rencana keamanan fisik lokasi yang terdokumentasi.
	The Vendor shall verify and provide documentation that enclosures such as walls, buildings, or fences adequately secure the perimeter against pedestrian, vehicular, and projectile intrusion.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa pelindung seperti dinding, bangunan, atau pagar cukup mengamankan *perimeter* terhadap intrusi pejalan kaki, kendaraan, dan proyektil.

The Vendor shall allow access within the perimeter only to those employees, contractors, or guests cleared by both Vendor and Purchaser.	Vendor akan mengizinkan akses di dalam *perimeter* hanya untuk karyawan, kontraktor, atau tamu yang diizinkan oleh Vendor dan Pembeli.
The Vendor shall verify and provide documentation that all employed guards have completed background checks.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa semua karyawannya telah dilakukan pemeriksaan tentang latar belakangnya.
The Vendor shall coordinate with local authorities when installing and using remote alarm systems. The Vendor shall provide non-reproducible keys or keycards for all locks.	Vendor harus berkoordinasi dengan pihak berwenang setempat saat memasang dan menggunakan sistem alarm jarak jauh. Vendor harus menyediakan kunci atau kartu kunci yang tidak dapat direproduksi untuk semua kunci.
The Vendor shall verify and provide documentation that security features do not hamper operations.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa fitur keamanan tidak menghambat operasi.
The Vendor shall verify and provide documentation that monitoring and alarm of physical access can be separated from the control network.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa pemantauan dan alarm akses fisik dapat dipisahkan dari jaringan kontrol.
9.8.3. Manual Override Control.	9.8.3. Kontrol *Override* Manual.
The Vendor shall provide the means to physically secure the Manual Control Mechanism (MCM), whether through a lockable enclosure or locking functionality built into the MCM itself.	Vendor harus menyediakan sarana untuk secara fisik mengamankan Mekanisme Kontrol Manual (*MCM*), baik melalui *enclosure* yang dapat dikunci atau fungsionalitas penguncian yang ada di dalam *MCM* itu sendiri.
The Vendor shall provide two non-reproducible keys to all locking MCMs.	*Vendor* harus menyediakan dua kunci yang tidak dapat direproduksi untuk semua *MCM* yang terkunci.
The Vendor shall change all locks, locking codes, keycards, and any other keyed entrances according to a 2-weeks period.	*Vendor* harus mengganti semua kunci, kode pengunci, kartu kunci, dan pintu masuk lainnya dengan fasilitas kunci yang sesuai kebutuhan

	dalam periode 2 minggu.
9.8.4. Intra-perimeter Communications.	9.8.4. Komunikasi *Intra Perimeter*.
The Vendor shall verify and provide documentation that physical communication channels are secured from physical intrusion.	*Vendor* harus melakukan verifikasi dan memberikan dokumentasi bahwa saluran komunikasi fisik diamankan dari gangguan fisik.
The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa jangkauan komunikasi nirkabel terbatas di dalam *perimeter*.
The Vendor shall verify and provide documentation that communication channels are as direct as possible.	*Vendor* harus melakukan verifikasi dan memberikan dokumentasi bahwa saluran komunikasi selangsung mungkin.
9.9 Network Partitioning	9.9 Partisi Jaringan
9.9.1. Network Device	9.9.1. Perangkat Jaringan.
The Vendor shall conform to ISA-99 / IEC-62443 standard unless otherwise stated and documented, with deviations properly recorded and agreed upon by the OWNER.	*Vendor* harus memenuhi standar ISA-99 / IEC-62443 kecuali dinyatakan lain dan didokumentasikan, dengan penyimpangan yang dicatat dengan benar dan disetujui oleh PEMILIK.
The Vendor shall provide a method for managing the network devices and changing addressing schemes.	Vendor harus menyediakan metode untuk mengelola perangkat jaringan dan mengubah skema pengalamatan.
The Vendor shall verify and provide documentation that the network configuration management interface is secured.	Vendor harus melakukan verifikasi dan memberikan dokumentasi bahwa antarmuka manajemen konfigurasi jaringan diamankan.
The Vendor shall provide ACLs, port security address lists, and enhanced security for the port mirroring.	Vendor harus menyediakan *ACL,* daftar alamat keamanan port, dan keamanan yang ditingkatkan untuk pencerminan port.
The Vendor shall remove or disable unused network configuration and management functions on the network devices.	*Vendor* harus menghapus atau menonaktifkan konfigurasi jaringan dan fungsi manajemen yang tidak digunakan pada perangkat jaringan.
The Vendor shall provide firewall rules for inbound and outbound	Vendor harus menyediakan aturan *firewall* untuk lalu lintas masuk dan

traffic based on deny-all rule sets.	keluar berdasarkan aturan yang berdasarkan semua ditolak (deny-all).
The Vendor shall provide NIDS rules and log review tools that verify the function of the firewall and detect anomalous traffic.	Vendor harus menyediakan aturan *NIDS* dan alat tinjauan *log* yang memverifikasi fungsi *firewall* dan mendeteksi lalu lintas yang tidak wajar.
The Vendor shall provide a NIPS architecture that will work with the communication method. The Vendor shall provide VPN concentrators configured with filters and port security.	Vendor harus menyediakan arsitektur *NIPS* yang akan bekerja dengan metode komunikasi. Vendor harus menyediakan konsentrator *VPN* yang dikonfigurasi dengan filter dan keamanan port.
Post-contract award, the Vendor shall provide documentation on the network devices installed with security settings.	Paska kontrak, Vendor harus menyediakan dokumentasi pada perangkat jaringan yang dipasang dengan pengaturan keamanan.
9.9.2. Network Architecture.	9.9.2. Arsitektur Jaringan
The Vendor shall follow ISA-99 / IEC-62443 Network Design, and document any deviation. Such deviations are allowed only when approved in writing by Purchaser.	Vendor harus mengikuti Desain Jaringan ISA-99 / IEC-62443, dan mendokumentasikan setiap penyimpangan. Penyimpangan tersebut hanya diperbolehkan jika disetujui secara tertulis oleh Pembeli.
The Vendor shall provide and document secure network architecture where the higher security zones originate communication to less secure zones.	Vendor harus menyediakan dan mendokumentasikan arsitektur jaringan yang aman di mana zona keamanan yang lebih tinggi berasal dari komunikasi ke zona yang kurang aman.
The Vendor shall provide and document the design for all communication paths between networks of different security zones through a DMZ.	Vendor harus menyediakan dan mendokumentasikan desain untuk semua jalur komunikasi antara jaringan zona keamanan yang berbeda melalui *DMZ*.
The Vendor shall verify and document that disconnection points are established between the network partitions and provide the methods to isolate subnets to continue limited operations.	Vendor harus melakukan verifikasi dan mendokumentasikan bahwa titik pemutusan dibuat antara partisi jaringan dan menyediakan metode untuk mengisolasi *subnet* untuk melanjutkan operasi terbatas.

The Vendor shall provide and document tailored filtering and monitoring rules for all security zones and alarm for unexpected traffic.	Vendor harus menyediakan dan mendokumentasikan aturan penyaringan dan pemantauan yang disesuaikan untuk semua zona keamanan dan alarm untuk lalu lintas yang tidak terduga.
The Vendor shall provide and document a DMZ that is restricted to communications where all traffic is monitored, alarmed, and filtered.	Vendor harus menyediakan dan mendokumentasikan *DMZ* yang dibatasi untuk komunikasi di mana semua lalu lintas dipantau, diperingatkan, dan disaring.
The Vendor shall provide and document outbound filtering and alarms for unexpected traffic through security zones.	Vendor harus menyediakan dan mendokumentasikan pemfilteran keluar dan alarm untuk lalu lintas tak terduga melalui zona keamanan.
The Vendor shall define all sources and destinations with enforced communication origination even during restart conditions between security zones.	Vendor harus menetapkan semua sumber dan tujuan dengan asal komunikasi yang dipaksakan bahkan selama kondisi restart antara zona keamanan.
The Vendor shall provide and document dual DMZ architectures using different products performing the same functionality running in parallel.	Vendor harus menyediakan dan mendokumentasikan arsitektur *DMZ* ganda menggunakan produk berbeda yang menjalankan fungsi yang sama secara paralel.
The Vendor shall provide and document a mechanism for patching a single DMZ architecture running in a parallel configuration without disruption to the other DMZ running in parallel.	Vendor harus menyediakan dan mendokumentasikan mekanisme untuk proses *patch* arsitektur *DMZ* tunggal yang berjalan dalam konfigurasi paralel tanpa mengganggu *DMZ* lain yang berjalan secara paralel.
Post-contract award, the Vendor shall provide network architecture documentation.	Paska kontrak, Vendor harus menyediakan dokumentasi arsitektur jaringan.
9.10 Wireless Technologies	9.10 Teknologi nirkabel
9.10.1. Bluetooth Technology.	9.10.1. Teknologi *Bluetooth*
When providing a Bluetooth-enabled device, the vendor shall meet the Bluetooth specification	Saat menyediakan perangkat yang mempunyai fasilitas *Bluetooth*, vendor harus memenuhi spesifikasi

and the related documentation.	*Bluetooth* dan dokumentasi terkait.
Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the Bluetooth-enabled device to communicate with the control network, including other wireless equipment that can communicate with the Vendor-supplied device.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan untuk perangkat berkemampuan *Bluetooth* untuk berkomunikasi dengan jaringan kontrol, termasuk peralatan nirkabel lain yang dapat berkomunikasi dengan perangkat yang dipasok *Vendor*.
The Vendor shall provide documentation on the range of the Bluetooth-enabled device, power requirements, and the designated frequency of operation for each device.	*Vendor* harus memberikan dokumentasi tentang jangkauan perangkat berkemampuan *Bluetooth,* kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
The Vendor shall define interoperability limits for the Bluetooth-enabled device. This includes specifying what equipment the Bluetooth-enabled device could replace, what additional hardware or software is required to make the replacement, and any problems or limitations that may be introduced. Limitations related to new functionality being introduced into the control system must also be specified.	*Vendor* harus menetapkan batas interoperabilitas untuk perangkat berkemampuan *Bluetooth*. Ini termasuk menentukan peralatan apa yang dapat diganti oleh perangkat berkemampuan *Bluetooth,* perangkat keras atau perangkat lunak tambahan apa yang diperlukan untuk melakukan penggantian, dan masalah atau batasan apa pun yang mungkin muncul. Batasan yang terkait dengan fungsionalitas baru yang diperkenalkan ke dalam sistem kontrol juga harus ditentukan.
The Vendor shall provide, within 3 weeks, any test data with analysis associated with the Bluetooth-enabled device.	Vendor dalam waktu 3 minggu harus menyediakan data uji apa pun dengan analisis yang terkait dengan perangkat berkemampuan Bluetooth.
The Bluetooth-enabled device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized access, modification	Perangkat berkemampuan Bluetooth harus dilengkapi dengan perangkat keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari akses,

	or use. The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.	modifikasi, atau penggunaan yang tidak sah. *Vendor* harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi Vendor atau manufaktur.
	The Vendor shall identify the configuration control options that enable varying of the security level of the device.	Vendor harus mengidentifikasi opsi kontrol konfigurasi yang memungkinkan berbagai tingkat keamanan perangkat.
	The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.	Vendor harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT.*
	The Vendor shall provide the Purchaser SAT procedures, which include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli, yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
	The quality of the implementation of the Bluetooth specification may vary from manufacturer to manufacturer (i.e. all Bluetooth implementations are not the same). The Vendor shall provide test data showing that basic attacks, such as malformed packet injection, do not cause the receiving Bluetooth device to crash, hang, or otherwise malfunction.	Kualitas implementasi spesifikasi *Bluetooth* dapat berbeda dari satu manufaktur ke manufaktur lainnya (yaitu semua implementasi *Bluetooth* kemungkinan tidak sama). *Vendor* harus menyediakan data uji yang menunjukkan bahwa serangan dasar, seperti injeksi paket yang salah, tidak menyebabkan perangkat *Bluetooth* penerima tidak sukses, *hang*, atau malfungsi.
9.10.2.	Wireless Closed-Circuit TV Technology (WCCTV).	9.10.2. Teknologi CCTV Nirkabel (WCCTV).
	The Vendor shall provide the WCCTV system and associated documentation.	Vendor harus menyediakan sistem WCCTV dan dokumentasi terkait.
	Post-contract award, the Vendor shall provide specific protocols and	Penyerahan pasca-kontrak, Vendor harus menyediakan protokol khusus

	other detailed information required for the WCCTV to communicate with the control network, including other wireless equipment that can communicate with the WCCTV.	dan informasi terperinci lainnya yang diperlukan agar WCCTV dapat berkomunikasi dengan jaringan kontrol, termasuk peralatan nirkabel lain yang dapat berkomunikasi dengan WCCTV.
	The Vendor shall provide documentation on the range of the WCCTV, power requirements, and the designated frequency of operation for each device.	*Vendor* harus memberikan dokumentasi tentang jangkauan WCCTV, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
	The Vendor shall provide, within 2 weeks, any test data with analysis associated with the mobile radio.	*Vendor* dalam waktu 2 minggu harus menyediakan data uji apa pun dengan analisis yang terkait dengan radio bergerak.
	The Vendor shall provide the Purchaser SAT procedures that include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
	The Vendor shall document the equipment configuration.	*Vendor* harus mendokumentasikan konfigurasi peralatan.
	The vendor shall provide configuration specifications for implementing encryption and authentication between the cameras and the network and specifically note all security measures associated with the system.	*Vendor* harus menyediakan spesifikasi konfigurasi untuk menerapkan enkripsi dan otentikasi antara kamera dan jaringan dan secara khusus mencatat semua tindakan keamanan yang terkait dengan sistem.
	The Vendor shall provide multiple levels of Quality of Service (QoS) that enable customization for specific mission-critical applications.	Vendor harus menyediakan berbagai tingkat kualitas layanan *(QoS)* yang memungkinkan penyesuaian untuk aplikasi misi kritikal tertentu.
	The Vendor shall provide advanced video compression techniques, such as MPEG4 and H.264, which can dramatically reduce the bandwidth requirements for video.	Vendor harus menyediakan teknik kompresi video tingkat lanjut, seperti *MPEG4* dan *H.264* yang dapat mengurangi secara luar biasa kebutuhan *bandwidth* untuk video.
9.10.3.	Radio Frequency Identification	9.10.3. Teknologi Identifikasi Frekuensi

Technology (RFID).	Radio (RFID).
The Vendor shall provide the RFID system and associated documentation.	Vendor harus menyediakan sistem *RFID* dan dokumentasi terkait.
Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the RFID device to communicate with the control network, including other wireless equipment that can communicate with the Vendor-supplied device.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan oleh perangkat *RFID* untuk berkomunikasi dengan jaringan kontrol termasuk peralatan nirkabel lain yang dapat berkomunikasi dengan perangkat yang dipasok *Vendor*.
The Vendor shall provide documentation on the range of the RFID device and power requirements.	*Vendor* harus menyediakan dokumentasi tentang jangkauan perangkat *RFID* dan kebutuhan daya.
The Vendor shall provide, within 2weeks, any test data with analysis associated with the RFID system.	*Vendor* dalam waktu 2 minggu harus menyediakan data uji apa pun dengan analisis yang terkait dengan sistem *RFID.*
The RFID system shall provide encryption of radio signals. The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.	Sistem *RFID* harus menyediakan enkripsi sinyal radio. *Vendor* harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall provide the Purchaser SAT procedures that include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).	Vendor harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.).
The Vendor shall identify how eavesdropping, MitM, and DoS	Vendor harus mengidentifikasi bagaimana *eavesdropping, MitM*,

attacks, including spoofing and power attacks, are mitigated with their technology.

dan serangan *DoS,* termasuk *spoofing* dan serangan power, dimitigasi dengan teknologi mereka.

9.10.4. 802.11 Technology (Wi-Fi).

There is only one current 802.11 standard. It is denoted by IEEE 802.11 followed by the date that it was published. The standard is updated by means of amendments. When a wireless device is referred to as 802.11x, x is an amendment to the original 802.11 standard. As of this date, IEEE 802.11-2007 is the most current 802.11 document available and contains cumulative changes (802.11a, b, d, e, g, h, i, j) from multiple sub-letter task groups. Care must be exercised when defining the 802.11 standard in procurement documents to be sure of the latest version.

The 802.11 standard, hereafter referred to as 802.11, defines the MAC and physical layers for a LAN with wireless connectivity where the connected devices are within close proximity to each other.

The Basic Service Set is the basic component of an 802.11 wireless LAN. The Basic Service Set consists of a group of stations. The station is the basic component of the WLAN. It is any device that provides the 802.11 protocol (MAC, physical layers, and a connection to the wireless device). The station might be a personal computer, handheld device, or an access point and may be mobile or stationary.

Security is provided by encryption, authentication, and configuration

9.10.4. Teknologi 802.11 (Wi-Fi).

Hanya ada satu standar 802.11 saat ini. Hal ini dilambangkan dengan IEEE 802.11 diikuti dengan tanggal yang diterbitkan. Standar diperbarui melalui amandemen. Ketika perangkat nirkabel disebut sebagai 802.11x, x adalah amandemen terhadap standar 802.11 yang asli. Pada tanggal ini, IEEE 802.11-2007 adalah dokumen 802.11 terbaru yang tersedia dan berisi perubahan kumulatif (802.11a, b, d, e, g, h, i, j) dari beberapa kelompok tugas sub-huruf. Kehati-hatian harus dilakukan ketika mendefinisikan standar 802.11 dalam dokumen pengadaan untuk memastikan versi terbaru.

Standar 802.11, selanjutnya disebut 802.11, mendefinisikan *MAC* dan lapisan fisik untuk *LAN* dengan konektivitas nirkabel di mana perangkat yang terhubung berada dalam jarak dekat satu sama lain.

Basic Service Set adalah komponen dasar dari *LAN* nirkabel 802.11. *Basic Service Set* terdiri dari sekelompok stasiun. Stasiun adalah komponen dasar dari *WLAN*. Ini adalah perangkat apa pun yang menyediakan protokol 802.11 (*MAC*, lapisan fisik, dan koneksi ke perangkat nirkabel). Stasiun dapat berupa komputer pribadi, perangkat genggam, atau titik akses dan dapat bergerak atau tidak bergerak.

Keamanan disediakan oleh enkripsi, otentikasi, dan kontrol konfigurasi.

control. The encryption methods used are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2. WEP can be easily intercepted and decoded. Numerous free software tools exist to aid in such endeavors. Due to these weaknesses, enhanced security was introduced for Wireless Fidelity (Wi-Fi) networks through the WPA protocol. The security of connections using this protocol depends largely on the strength of the user-supplied pass-phrase. Free software and descriptions of how to attack these connections also are available online. Improving upon previous security implementations, the Wi-Fi Alliance released the WPA2 standard, which uses a stronger encryption algorithm.

Metode enkripsi yang digunakan adalah *Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA),* atau *WPA2. WEP* dapat dengan mudah dicegat dan diterjemahkan. Banyak perangkat lunak bebas tersedia untuk membantu upaya tersebut. Karena kelemahan ini, keamanan yang ditingkatkan diperkenalkan untuk jaringan *Wireless Fidelity (Wi-Fi)* melalui protokol *WPA.* Keamanan koneksi yang menggunakan protokol ini sangat bergantung pada kekuatan frasa sandi yang disediakan pengguna. Perangkat lunak gratis dan deskripsi tentang cara menyerang koneksi ini juga tersedia secara online. Meningkatkan implementasi keamanan sebelumnya, *Wi-Fi* Alliance merilis standar *WPA2*, yang menggunakan algoritma enkripsi yang lebih kuat.

Despite the availability of strong encryption for user communication, the management frames of IEEE 802.11 messages are not encrypted, leaving the door open for DoS attacks. Several tools are available that can cause users to drop off the network or send messages to hamper the functionality of wireless end points. Such tools include Wi-Fi jammers, designed to block IEEE 802.11 transmissions, and rogue access points, that are set up in hopes of attracting connections then stealing sensitive information or altering communications. Adding to and enabling attacks is the fact that Wi-Fi access points are often set up quickly and without security

Terlepas dari ketersediaan enkripsi yang kuat untuk komunikasi pengguna, kerangka manajemen pesan IEEE 802.11 tidak dienkripsi, membiarkan pintu terbuka untuk serangan *DoS*. Beberapa alat tersedia yang dapat menyebabkan pengguna memutuskan jaringan atau mengirim pesan untuk menghambat fungsionalitas titik akhir nirkabel. Alat tersebut termasuk *jammer Wi-Fi*, yang dirancang untuk memblokir transmisi IEEE 802.11, dan titik akses jahat yang dipasang dengan harapan menarik koneksi kemudian mencuri informasi sensitif atau mengubah komunikasi. Menambah dan mengaktifkan serangan adalah fakta bahwa titik akses Wi-Fi sering

foresight. This results in the use of weak or no encryption, allowing attackers to impersonate wireless end points in hopes of providing false data. It also may result in users not changing default passwords for device management, allowing attackers to gain full control of the access point as default passwords are common knowledge. Recently, researchers have considered the possibility of worms that use the aforementioned security weaknesses to propagate on the local network. Such malicious code would rely on two assumptions to propagate. First, in urban settings, numerous Wi-Fi networks exist within close proximity of one another. Second, that victim machines are configured to connect to multiple networks.

kali diatur dengan cepat dan tanpa tinjauan keamanan. Hal ini mengakibatkan penggunaan enkripsi yang lemah atau tanpa enkripsi, memungkinkan penyerang untuk meniru titik akhir nirkabel dengan harapan memberikan data palsu. Ini juga dapat mengakibatkan pengguna tidak mengubah kata sandi default untuk manajemen perangkat, memungkinkan penyerang untuk mendapatkan kontrol penuh dari titik akses karena kata sandi default adalah pengetahuan umum. Baru-baru ini, para peneliti telah mempertimbangkan kemungkinan *worm* yang menggunakan kelemahan keamanan yang disebutkan di atas untuk menyebar di jaringan lokal. Kode berbahaya semacam itu akan bergantung pada dua asumsi untuk disebarkan. Pertama, di lingkungan perkotaan, banyak jaringan *Wi-Fi* ada dalam jarak dekat satu sama lain. Kedua, mesin korban dikonfigurasi untuk terhubung ke beberapa jaringan.

9.10.5. ZigBee Technology.

The Vendor shall design and provide a configured ZigBee wireless network, meeting the requirements of the ZigBee specification, and associated documentation and running on a licensed frequency. The Vendor shall configure the ZigBee network such that the following conditions are met:

- The ZigBee network infrastructure shall be protected with a Network Key.

9.10.5. Teknologi *ZigBee*.

Vendor harus merancang dan menyediakan jaringan nirkabel *ZigBee* yang dikonfigurasi untuk memenuhi persyaratan spesifikasi *ZigBee* dan dokumentasi terkait serta berjalan pada frekuensi yang berlisensi. *Vendor* harus mengkonfigurasi jaringan *ZigBee* sedemikian rupa sehingga kondisi berikut terpenuhi:

- Infrastruktur jaringan *ZigBee* harus dilindungi dengan Kunci Jaringan.

• Address filtering shall be employed at the MAC layer.	• Penyaringan alamat harus diterapkan pada lapisan *MAC.*
• The ZigBee encryption security service shall be utilized.	• Layanan keamanan enkripsi *ZigBee* harus digunakan.
• Source node authentication shall be implemented.	• Otentikasi node asal harus diimplementasikan.
• A personal area network (PAN) Identifier shall be preassigned and node connectivity shall be restricted.	• Pengidentifikasi jaringan area pribadi (*PAN*) harus ditetapkan sebelumnya dan konektivitas simpul harus dibatasi.
• Out-of-band key loading method shall be used.	• Metode pemuatan kunci *out-of-band* harus digunakan.
• Layer-2 security mechanisms supported in the IEEE 802.15.4 lower layer MAC shall be enabled.	• Mekanisme keamanan lapisan-2 yang didukung dalam MAC lapisan bawah IEEE 802.15.4 harus diaktifkan.
• Secure network admission control shall be implemented.	• Kontrol penerimaan jaringan yang aman harus diterapkan.
• Nodes with the Trust Center address shall be preconfigured.	• Node dengan alamat Pusat *Trust Center* harus dilakukan prakonfigurasi.
Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the LR-WPAN device to communicate with the control network, including other wireless equipment that can communicate with the vendor-supplied device.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan untuk perangkat *LR-WPAN* untuk berkomunikasi dengan jaringan kontrol, termasuk peralatan nirkabel lain yang dapat berkomunikasi dengan perangkat yang dipasok vendor.
The Vendor shall provide documentation on the range of the LR-WPAN device, power requirements, and the designated frequency of operation for each device.	Vendor harus memberikan dokumentasi tentang jangkauan perangkat *LR-WPAN,* kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.

The Vendor shall allow and recommend alarm settings in accordance to the needs of the system.	Vendor harus mengizinkan dan merekomendasikan pengaturan *alarm* sesuai dengan kebutuhan sistem.
The Vendor shall define interoperability limits for the LR-WPAN device specifically stating the devices the LR-WPAN device could replace and any associated problems that might be associated with the replacement.	Vendor harus menetapkan batas interoperabilitas untuk perangkat *LR-WPAN* yang secara khusus menyatakan perangkat yang dapat diganti oleh perangkat *LR-WPAN* dan masalah terkait yang mungkin terkait dengan penggantian tersebut.
The Vendor shall provide, within 2 weeks, any test data h with analysis associated with the LR-WPAN device.	Vendor dalam waktu 2 minggu harus menyediakan setiap data uji dengan analisis yang terkait dengan perangkat *LR-WPAN*.
LR-WPAN device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.	Perangkat *LR-WPAN* harus dilengkapi dengan perangkat keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari modifikasi atau penggunaan yang tidak sah. *Vendor* harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall provide the LR-WPAN device with the standard security measures as specified in the ZigBee standard.	*Vendor* harus menyediakan perangkat *LR-WPAN* dengan langkah-langkah keamanan standar sebagaimana ditentukan dalam standar *ZigBee.*
The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.	*Vendor* harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat

sebelum *FAT*.

The Vendor shall provide the Purchaser SAT procedures that include exercising all functionality and calibration procedures.

Vendor harus menyediakan prosedur *SAT* Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.

The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

Vendor harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.).

The Vendor shall identify the configuration control options that enable varying of the security level of the device.

Vendor harus mengidentifikasi opsi konfigurasi kontrol yang memungkinkan berbagai tingkat keamanan perangkat.

9.10.6. WirelessHART Technology.

9.10.6. Teknologi *WirelessHART.*

The Vendor shall provide, within 2 weeks, any test data with analysis associated with the WirelessHART devices, using the latest revision of the WirelessHART protocol version 7 or latest.

Vendor dalam waktu 2 minggu harus menyediakan data uji apa pun dengan analisis yang terkait dengan perangkat *WirelessHART*, menggunakan revisi terbaru dari protokol *WirelessHART* versi 7 atau terbaru.

The WirelessHART device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.

Perangkat *WirelessHART* harus dilengkapi dengan perangkat keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari modifikasi atau penggunaan yang tidak sah. Vendor harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.

The Vendor shall provide the WirelessHART device with the standard security measures as specified in the WirelessHART

Vendor harus menyediakan perangkat *WirelessHART* dengan langkah-langkah keamanan standar sebagaimana ditentukan dalam

	standard.	standar *WirelessHART.*
	The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.	*Vendor* harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*.
	The Vendor shall provide the Purchaser SAT procedures that include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
	The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).	*Vendor* harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.).
9.10.7.	Mobile Radios.	9.10.7. Radio Seluler.
	The Vendor shall provide the wireless mobile radio device and associated documentation.	Vendor harus menyediakan perangkat radio seluler nirkabel dan dokumentasi terkait.
	Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the mobile radio to communicate with the control network, including other wireless equipment that can communicate with the Vendor-supplied device.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan untuk radio bergerak untuk berkomunikasi dengan jaringan kontrol, termasuk peralatan nirkabel lain yang dapat berkomunikasi dengan perangkat yang dipasok *Vendor*.
	The Vendor shall provide documentation on the range of the mobile radio, power requirements, and the designated frequency of operation for each device.	*Vendor* harus memberikan dokumentasi tentang jangkauan radio bergerak, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
	The Vendor shall provide, within a pre-negotiated period, any test data with analysis associated with the mobile radio.	*Vendor* dalam periode pra-negosiasi harus menyediakan setiap data uji dengan analisis yang terkait dengan radio bergerak.

	The mobile radio shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.	Radio bergerak harus dilengkapi dengan perangkat keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari modifikasi atau penggunaan yang tidak sah. *Vendor* harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.
	The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.	*Vendor* harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*.
	The Vendor shall provide the Purchaser SAT procedures, that include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli, yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
	The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).	*Vendor* harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.).
9.10.8.	Wireless Mesh Network Technology.	9.10.8. Teknologi Jaringan *Mesh* Nirkabel.
	The Vendor shall provide the wireless meshed network (WMN), meeting the requirements of the required sections of IEEE 802.11, and associated documentation.	Vendor harus menyediakan jaringan *mesh* nirkabel (WMN), memenuhi persyaratan dari IEEE 802.11, dan dokumentasi terkait.
	Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the WMN to communicate with the control network, including any other equipment that can	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi terperinci lainnya yang diperlukan agar *WMN* dapat berkomunikasi dengan jaringan kontrol, termasuk peralatan lain yang dapat berkomunikasi dengan

communicate with the WMN.	*WMN.*
The Vendor shall provide documentation on the range of the WMN device, power requirements, and the designated frequencies of operation for each device.	Vendor harus memberikan dokumentasi tentang jangkauan perangkat *WMN*, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
The Vendor shall allow and recommend alarm settings in accordance to the needs of the system.	Vendor harus mengizinkan dan merekomendasikan pengaturan *alarm* sesuai dengan kebutuhan sistem.
The Vendor shall define interoperability limits for the WMN device specifically stating the devices that could be replaced and any related problems that might be associated with the replacement.	Vendor harus menetapkan batas interoperabilitas untuk perangkat *WMN* yang secara khusus menyatakan perangkat yang dapat diganti dan masalah terkait yang mungkin terkait dengan penggantian.
The Vendor shall provide, within 2 weeks, any test data with analysis associated with the WMN device.	Vendor dalam waktu 2 minggu harus menyediakan semua data uji dengan analisis yang terkait dengan perangkat *WMN*.
Each WMN device shall be provided with security mechanisms, such as passwords or security codes, to protect the device from unauthorized modification or use. The Vendor shall clearly identify these mechanisms and methods to change them from the Vendor-configured or manufacture default conditions.	Setiap perangkat *WMN* harus dilengkapi dengan mekanisme keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari modifikasi atau penggunaan yang tidak sah. Vendor harus dengan jelas mengidentifikasi mekanisme dan metode ini untuk mengubahnya dari kondisi default yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall provide the WMN device with the standard security measures as specified in the 802.11 standard and support the required level of encryption.	*Vendor* harus menyediakan perangkat *WMN* dengan langkah-langkah keamanan standar sebagaimana ditentukan dalam standar 802.11 dan mendukung tingkat enkripsi yang diperlukan.
The Vendor shall remove or disable all software artifacts that are not required for the operation and	Vendor harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak

maintenance of the device prior to the FAT.	diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*.
The Vendor shall provide the Purchaser SAT procedures which include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur *SAT* Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
The Vendor shall identify the configuration control options that enable varying of the security level of the device.	*Vendo*r harus mengidentifikasi opsi kontrol konfigurasi yang memungkinkan berbagai tingkat keamanan perangkat.
The Vendor shall demonstrate that cooperative WMN nodes can distinguish jamming from channel saturation and provide operational alerts.	*Vendor* harus menunjukkan bahwa node *WMN* kooperatif dapat membedakan *jamming* dari saturasi saluran dan memberikan peringatan operasional.
The Vendor shall provide test data showing that basic attacks, such as malformed packet injection, do not cause the WMN device to crash, hang, or otherwise malfunction.	*Vendor* harus menyediakan data uji yang menunjukkan bahwa serangan dasar, seperti injeksi paket yang salah, tidak menyebabkan perangkat *WMN* bertabrakan, *hang*, atau malfungsi.
9.10.9. Cellular Technology.	9.10.9. Teknologi Seluler.
The Vendor shall provide the cellular system equipment and associated documentation.	Vendor harus menyediakan peralatan sistem seluler dan dokumentasi terkait.
Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the cellular system to communicate with the control network, including other equipment that can communicate with the cellular system.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi terperinci lainnya yang diperlukan agar sistem seluler dapat berkomunikasi dengan jaringan kontrol, termasuk peralatan lain yang dapat berkomunikasi dengan sistem seluler.
The Vendor shall provide documentation on the range of the cellular system, power requirements, and the designated frequency of operation for each device.	*Vendor* harus memberikan dokumentasi tentang jangkauan sistem seluler, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.

The Vendor shall provide, within 2 weeks, any test data with analysis associated with the cellular system.	*Vendor* harus menyediakan dalam waktu 2 minggu, data uji apa pun dengan analisis yang terkait dengan sistem seluler.
The Vendor shall provide the Purchaser SAT procedures, which include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur SAT Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection,).	*Vendor* harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi,).
9.10.10. WiMAX Technology.	9.10.10. Teknologi *WiMAX*
The Vendor shall provide the WiMAX subscriber station equipment and associated documentation.	*Vendor* harus menyediakan peralatan stasiun pelanggan *WiMAX* dan dokumentasi terkait.
Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the WiMAX subscriber station to communicate with the base station, including other equipment that can communicate with the WiMAX subscriber station.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan untuk stasiun pelanggan *WiMAX* untuk berkomunikasi dengan stasiun pangkalan, termasuk peralatan lain yang dapat berkomunikasi dengan stasiun pelanggan *WiMAX*.
The Vendor shall provide documentation on the range of the WiMAX subscriber station, power requirements, and the designated frequency of operation for each device.	*Vendor* harus menyediakan dokumentasi tentang jangkauan stasiun pelanggan *WiMAX*, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
The Vendor shall provide, within 2 weeks, any test data with analysis associated with the WiMAX subscriber station to base station communications.	*Vendor* dalam waktu 2 minggu harus menyediakan setiap data uji dengan analisis yang terkait dengan komunikasi stasiun pelanggan *WiMAX* ke stasiun

		sumber.
	The Vendor shall clearly identify these security devices and methods to change them from the Vendor-configured or manufacture default conditions.	*Vendor* harus dengan jelas mengidentifikasi perangkat keamanan ini dan metode untuk mengubahnya dari kondisi bawaan yang dikonfigurasi *Vendor* atau manufaktur.
	The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.	*Vendor* harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat sebelum *FAT*.
	The Vendor shall provide the Purchaser SAT procedures that include exercising all functionality and calibration procedures.	*Vendor* harus menyediakan prosedur SAT Pembeli yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.
	The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).	*Vendor* harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.).
9.10.11.	Microwave and Satellite Technology.	9.10.11. Teknologi *Microwave* dan Satelit.
	The Vendor shall provide the microwave device, meeting the requirements of GR-63 NEBS and GR-1089, with associated documentation, and running on a licensed frequency.	*Vendor* harus menyediakan perangkat gelombang mikro, memenuhi persyaratan GR-63 NEBS dan GR-1089, dengan dokumentasi terkait, dan berjalan pada frekuensi berlisensi.
	Post-contract award, the Vendor shall provide specific protocols and other detailed information required for the microwave device to communicate with the control network, including other equipment that can communicate with the microwave device.	Penyerahan paska kontrak, Vendor harus menyediakan protokol khusus dan informasi rinci lainnya yang diperlukan untuk perangkat gelombang mikro untuk berkomunikasi dengan jaringan kontrol, termasuk perlengkapan lain yang dapat berkomunikasi

	dengan perangkat gelombang mikro.
The Vendor shall provide documentation on the range of the microwave device, power requirements, and the designated frequency of operation for each device.	Vendor harus memberikan dokumentasi tentang jangkauan perangkat gelombang mikro, kebutuhan daya, dan frekuensi operasi yang ditentukan untuk setiap perangkat.
The Vendor shall allow and recommend alarm settings in accordance to the needs of the system.	Vendor harus mengizinkan dan merekomendasikan pengaturan *alarm* sesuai dengan kebutuhan sistem.
The Vendor shall define interoperability limits for the microwave device specifically stating the devices that could be replaced and any problems that might be associated with the replacement.	*Vendor* harus menetapkan batas interoperabilitas untuk perangkat gelombang mikro yang secara khusus menyatakan perangkat yang dapat diganti dan masalah apa pun yang mungkin terkait dengan penggantian.
The Vendor shall provide, within 2 weeks, any test data with analysis associated with the microwave device.	*Vendor* dalam waktu 2 minggu harus menyediakan semua data uji dengan analisis yang terkait dengan perangkat gelombang mikro.
The microwave device shall be provided with security features, such as passwords or security codes, to protect the device from unauthorized modification or use. The Vendor shall clearly identify these security measures and the necessary methods to change them from the Vendor-configured or manufacture default conditions.	Perangkat gelombang mikro harus dilengkapi dengan fitur keamanan, seperti kata sandi atau kode keamanan, untuk melindungi perangkat dari modifikasi atau penggunaan yang tidak sah. *Vendor* harus dengan jelas mengidentifikasi langkah-langkah keamanan ini dan metode yang diperlukan untuk mengubahnya dari kondisi default yang dikonfigurasi *Vendor* atau manufaktur.
The Vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device	*Vendor* harus menghapus atau menonaktifkan semua artefak perangkat lunak yang tidak diperlukan untuk pengoperasian dan pemeliharaan perangkat

prior to the FAT.

The Vendor shall provide the Purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The Vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.). All information carried across the microwave links shall be secured through digital encryption

sebelum *FAT*.

Vendor harus menyediakan prosedur Pembeli, yang mencakup pelaksanaan semua fungsionalitas dan prosedur kalibrasi.

Vendor harus mendokumentasikan konfigurasi peralatan dan secara khusus mencatat setiap tindakan keamanan yang terkait dengan sistem (perangkat enkripsi, proteksi kata sandi, dll.). Semua informasi yang dibawa melalui tautan gelombang mikro harus diamankan melalui enkripsi digital.

9.11 Flaw Remediation

9.11.1. Notification and Documentation from ICSS Vendor.

Flaw remediation refers to the actions to be performed and documentation to be produced when flaws are discovered in control system software, hardware, and system architectures created by or under the control of the Vendor.

The Vendor shall have and provide documentation of a written flaw remediation process.

The Vendor shall provide appropriate software updates and/or workarounds to mitigate all vulnerabilities associated with the flaw within 2 weeks.

Post-contract award, after the Vendor is made aware of or discovers any flaws, the Vendor shall provide notification of such flaws affecting security of Vendor-

9.11 Perbaikan Cacat Produk

9.11.1. Pemberitahuan dan Dokumentasi dari *Vendor ICSS*

Perbaikan cacat produk mengacu pada tindakan yang harus dilakukan dan dokumentasi yang akan dihasilkan ketika kekurangan ditemukan dalam perangkat lunak sistem kontrol, perangkat keras, dan arsitektur sistem yang dibuat oleh atau di bawah kendali *Vendor*.

Vendor harus memiliki dan memberikan dokumentasi proses perbaikan cacat tertulis.

Vendor harus menyediakan pembaruan perangkat lunak yang sesuai dan/atau solusi untuk mengurangi semua kerentanan yang terkait dengan cacat dalam waktu 2 minggu.

Paska kontrak, setelah *Vendor* diberitahu atau menemukan kekurangan, Vendor harus memberikan pemberitahuan tentang kekurangan tersebut yang

supplied software within 3 weeks. Notification shall include, but is not limited to, detailed documentation describing the flaw with security impact, root cause, corrective actions, etc.

mempengaruhi keamanan perangkat lunak yang disediakan Vendor dalam waktu 3 minggu. Pemberitahuan harus mencakup tetapi tidak terbatas pada dokumentasi terperinci yang menjelaskan cacat dengan dampak keamanan, akar masalah, tindakan korektif, dll.

9.11.2. ICSS Problem Reporting.

Vulnerabilities exist in core logic and configuration of control systems. When flaws in software and/or hardware configuration are discovered by users, the Vendor shall have a process in place by which the user can report such flaws. A flaw remediation process shall be used to track progress of patches, fixes, and workarounds until completion.

9.11.2. Pelaporan Masalah *ICSS*

Kerentanan ada dalam logika inti dan konfigurasi sistem kontrol. Ketika kekurangan dalam konfigurasi perangkat lunak dan/atau perangkat keras ditemukan oleh pengguna, Vendor harus memiliki proses di mana pengguna dapat melaporkan kekurangan tersebut. Proses perbaikan cacat produk harus digunakan untuk melacak kemajuan *patch* dan perbaikan hingga selesai.

10. APPENDIXES

The interface sketches in the appendices below are only indicative. ICSS Contractor shall develop final interface drawings to show all required data, information and work process exchange, with the help from all the other contractors.

10. LAMPIRAN

Sketsa antarmuka dalam lampiran di bawah ini hanya indikatif. Kontraktor ICSS harus mengembangkan gambar antarmuka akhir untuk menunjukkan semua data, informasi dan pertukaran proses kerja yang diperlukan, dengan bantuan dari semua kontraktor lainnya.

APPENDIX 1. Typical Interfaces

LAMPIRAN 1. Antarmuka Tipikal

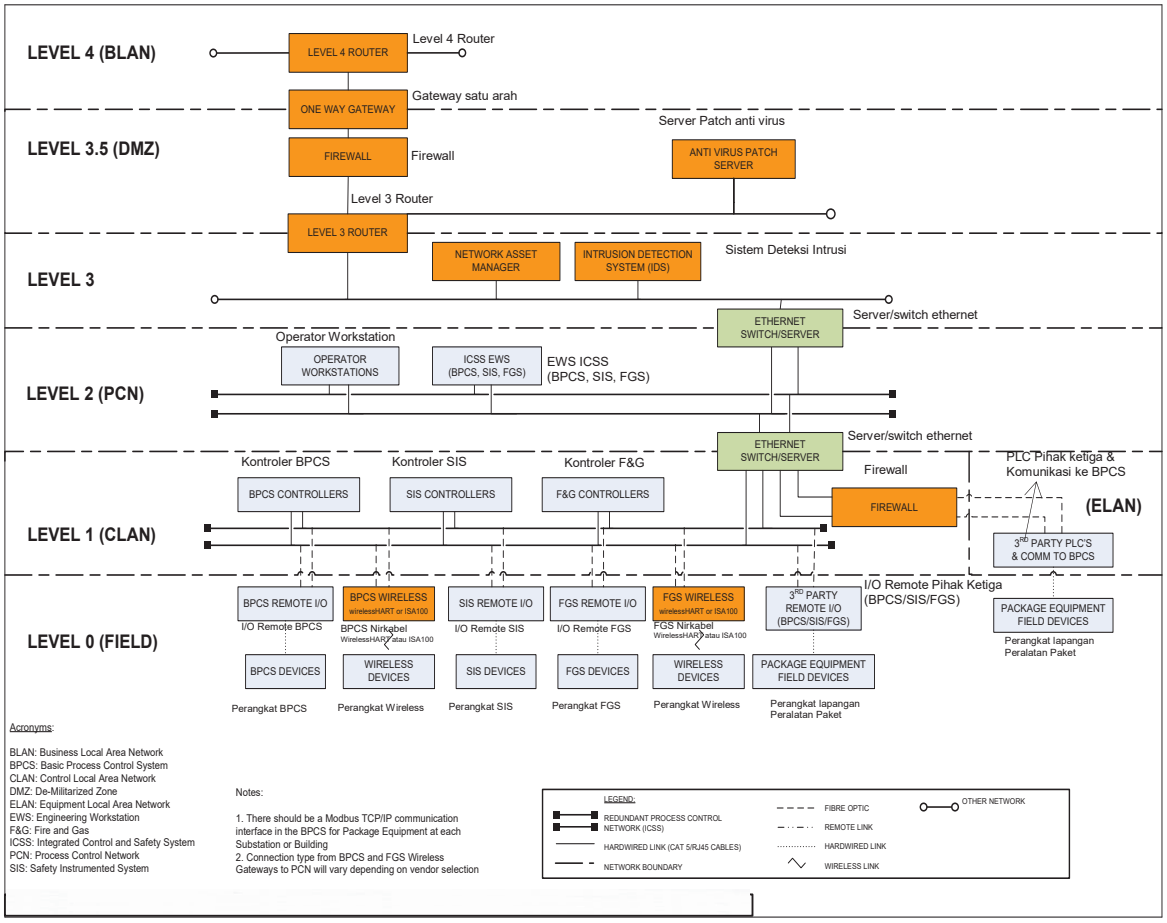

Figure 1. Non-inclusive example Network Diagram

Gambar 1. Diagram Jaringan contoh non-inklusif