Bank Resona Perdania

PEDOMAN HARDENING AS/400

HARDENING AS/400 GUIDELINE

Edisi ke-6, Maret 2023

6th Edition, March 2023

BOD Approval No 094/ITD/IT-PLN/IV/2023

DAFTAR ISI
Table of Content

Hal/*Page*

I. PENDAHULUAN

A. Latar Belakang

Mesin AS/400 digunakan untuk menjalankan aplikasi *Core Banking* Bank. Untuk itu dalam upaya mengelola penggunaannya, bank perlu membuat suatu pedoman untuk memastikan sistem beroperasi dengan aturan dan sistem keamanan yang berlaku, diantaranya membatasi akses dari *user* yang tidak berhak, mengurangi resiko kegagalan sistem, meminimalkan celah keamanan sistem dan melakukan monitoring atas aktifitas seluruh *user* yang menggunakan sistem. Dengan diperbaruinya pedoman ini dapat memberi rasa aman buat bank dan manajemen untuk menjamin aplikasi *core banking* dapat berjalan dengan stabil dan dikelola dengan baik.

B. Acuan

1. POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum;

2. SEOJK No.21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

   SEOJK No.21/POJK.03/2017 ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum

3. POJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum.

   Sejak 30 Oktober 2021, Pasal 20, Pasal 21, Pasal 22 dan Pasal 24 dalam POJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum dinyatakan dicabut dan tidak berlaku oleh POJK No. 13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum.

4. SEOJK No. 34/SEOJK.03/2016 tanggal 1 September 2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

I. INTRODUCTION

A. Background

AS/400 machine is used for running Bank Core Banking application. Then in effort to manage its use, the bank needs to make a guideline to ensure the system is operating with rules and systems applicable security, including limiting access of unauthorized use, reducing the risk of system failure, minimizes security system holes and monitoring the activities of entire user using the system. By renewing these guidelines may provide a sense of security for the bank and management to ensure the core banking applications can run stable and run well

B. Reference

1. POJK No.11/POJK.03/2022 concerning Application of Information Technology by Commercial Banks;

2. SEOJK No. 21/SEOJK.03/2017 about Implementation of Risk Management in the use of Information Technology by Public Bank.

   SEOJK No.21/POJK.03/2017 is declared to remain valid as long as it does not conflict with the provisions in POJK No.11/POJK.03/2022 concerning Implementation of Information Technology by Commercial Banks.

3. POJK No. 18/POJK.03/2016 about The application of Risk Management for Commercial Banks.

   Since October 30, 2021, Article 20, Article 21, Article 22 and Article 24 in POJK No. 18/POJK.03/2016 on the Implementation of Risk Management for Commercial Banks were declared revoked and invalid by POJK No. 13/POJK.03/2021 on the Implementation of Commercial Bank Products.

4. SEOJK No. 34/SEOJK.03/2016 at September 1, 2016 about The application of Risk Management for Commercial

5. Kebijakan Manajemen Risiko Teknologi Informasi.
6. Kebijakan Manajemen Risiko Secara Umum (Individual).
7. Kebijakan Hardening.
8. Kebijakan Manajemen Risiko Operasional.
9. Kebijakan Penggunaan Pihak Penyedia Jasa TI.
10. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi.
11. Kebijakan Manajemen Proyek dan Pengembangan Sistem.
12. Kebijakan Pengawasan Keamanan Sistem dan Informasi.
13. Kebijakan Audit Intern Teknologi Informasi.
14. Kebijakan Tugas dan Wewenang.
15. Kebijakan *Job Description*.
16. Kebijakan Komite Pengarah Teknologi Informasi.

C. Tujuan

1. Memastikan *setting*/konfigurasi sistem sudah memadai dan sesuai dengan kebijakan yang berlaku
2. Meminimalkan risiko yang diakibatkan kerentanan sistem pada sistem AS/400, seperti *user*, *service*, *protocol*, *file* dan program yang tidak digunakan atau perbedaan pengaturan pada mesin produksi dan backup
3. Memastikan perubahan dan perbaikan yang terjadi dapat dimonitor, diawasi dan dilakukan oleh personal yang bertanggung jawab
4. Untuk tertib administrasi dalam mempermudah pemeliharaan dan proses dikemudian hari.

Banks.

5. Information Technology Risk Management Policy.
6. Individual General Risk Management Policy.
7. Hardening Policy.
8. Operational Risk Management Policy.
9. The Use of IT Service Provider Policy.
10. Information Security and System Risk Management in the use of Information Technology Policy.
11. Project Management and System Development Policy.
12. System and Information Security Monitoring Policy.
13. Information Technology Internal Audit Policy.
14. Duties and Authorities Policy.
15. Job Description Policy.
16. Information Technology Steering Committee

D. Purpose

1. Ensure system setting / configuration is adwasuate and it accordance with applicable policies.
2. Minimize risk which caused of AS/400 system vulnerabilities in the system, such as user, service, protocol, files and programs that are no longer used or differences setting at production and backup machine.
3. Ensure the changes and improvements that occur can be monitored, supervised and carried out by responsible person.
4. To set good administration to ease the maintenance and process in the future

II. KETENTUAN UMUM

A. Definisi

1. *Hardening* merupakan proses atau metode untuk mengamankan sistem dari berbagai ancaman dan atau ketidak stabilan sistem dengan meminimalisasi risiko yang ada melalui setting/konfigurasi parameter-parameter yang tersedia.

2. *System Value* : adalah sekumpulan informasi yang dapat mempengaruhi lingkungan atau kerja sistem operasi AS/400.

3. *QSECOFR* : *User Id*. yang memiliki level tertinggi pada sistem AS/400. Dalam operasionalnya *user* tersebut dipegang dan diawasai penggunaannya oleh Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem.

4. Parameter: karakteristik atau fitur yang dapat membantu dalam mendefinisikan suatu sistem tertentu.

5. *Core Banking*: layanan yang disediakan oleh jaringan bank dimana nasabah dapat melakukan transaksi dari jaringan kantor bank tersebut.

6. Bank: PT. Bank Resona Perdania beserta seluruh kantor cabangnya diseluruh wilayah Republik Indonesia.

B. Pihak Terkait

1. Fungsi Operasi dan Dukungan TI

   1.1 Memelihara penggunaan user pada sistem AS/400.

   1.2 Melakukan Backup sistem AS/400 secara berkala.

   1.3 Memonitor dan memelihara kapasitas pada sistem AS/400 agar sistem berjalan sesuai dengan yang direncanakan.

II. GENERAL PROVISIONS

A. Definition

1. Hardening is a process or a method to secure a system from various threats and or instability of the system by minimize risk that exist through setting/ configuration available parameters.

2. System Value: is set of information that may affect at environement or process of AS/400 operating system.

3. QSECOFR: is User Id with highest level authority at AS/400 system. In operation the user is kept and monitored by Information Security and System Risk Controll Departement.

4. Parameter: is a characteristic or feature which can help in defining a particular system.

5. Core Banking: is services provide by a group of network bank branches where customer may do transactions from any member branch offices.

6. Bank: is PT. Bank Resona Perdania and its branches throughout the territory of Republic of Indonesia.

B. Related Party

1. IT Operation and Support Function

   1.1 Maintain use of the users on the AS/400 system.

   1.2 Perform regular AS/400 system backups.

   1.3 Monitor and maintain disk capacity of AS/400 system to ensure system runs as planned.

2. Departemen Sistem TI

2.1 Memastikan proses hardening sistem AS/400 sudah dilakukan sesuai dengan pedoman yang berlaku.

2.2 Memastikan proses perubahan hardening sistem AS/400 tidak mengganggu sistem Core Banking Bank yang berjalan.

2.3 Melakukan perbaikan dan atau peningkatan atas keamanan sistem yang ada sesuai dengan rekomendasi dan atau perkembangan teknologi yang ada.

2.4 Memastikan pengaturan dan konfigurasi pada mesin AS/400 produksi dan mesin AS/400 untuk Backup sama.

2.5 Mensosialisasikan perubahan pengaturan / konfigurasi yang terjadi dan dampaknya kepada Departemen Operasi TI dan Pengguna dalam hal perubahan yang dilakukan mengakibatkan perubahan pada penggunaan atau operasional harian.

3. Departemen Pengawas Keamanan Informasi Dan Risiko Sistem.

3.1 Melakukan monitoring dan evaluasi atas proses hardening yang dilakukan.

3.2 Melakukan evaluasi secara berkala, terhadap kelemahan dan keamanan sistem AS/400.

3.3 Memberikan rekomendasi kepada pihak terkait, hasil dari evaluasi diatas.

3.4 Memonitor pengguna dan aktifitas pengguna sistem AS/400, serta melaporkan hasil monitoring.

3.5 Memonitor penggunaan user QSECOFR sesuai dengan PEDOMAN PENGGUNAAN USER ID DAN PASSWORD USER ADMINISTRATOR, POWER USER, ROOT DAN QSECOFR.

2. IT System Departement

2.1 Ensure AS/400 system hardening process has been conducted in accordance with guidelines.

2.2 Ensure process of hardening AS/400 changes does not interfere to Bank Core Banking system which is running.

2.3 Make improvements or enhancement to existing security system in accordance with recommendations and or technolgies development.

2.4 Ensure setting and configuration on AS/400 machine at production and AS/400 machine Backup are same

2.5 Socialize changes on setting / configuration and their impact to IT Operation Departement and users in case the changes impacted to daily usage and operation.

3. Information Security And System Risk Departement.

3.1 Monitor and evaluate of hardening process which performed.

3.2 Conduct regular evaluation to AS/400 system weaknesses and security.

3.3 Provide recommendations to the relevant parties, the results of the evaluation above.

3.4 Monitoring users and users's activities in the AS/400 system, then report the monitoring result.

3.5 Monitoring usage of QSECOFR user accordance with ADMINISTRATOR USER, POWER USER, ROOT, and QSECOFR USER ID AND PASSWORD guidelines.

III. PROSEDUR

Proses instalasi akan dilakukan oleh pihak IBM atau rekan bisnis IBM. Setelah proses instalasi Bank akan melakukan konfigurasi sesuai dengan kebijakan Bank dan karaketeristik aplikasi yang akan digunakan. Untuk memastikan prosedur sudah dijalankan sesuai dengan yang ditentukan, maka digunakan suatu *checklist* yang berisikan hal-hal yang harus dipenuhi.

A. Ruang Lingkup

Ruang lingkup proses hardening sistem AS/400 meliputi :

1. Umum

   1.1. Koneksi sistem AS/400 ke/dari aplikasi-aplikasi lain hanya diperbolehkan untuk aplikasi-aplikasi unit produksi.

   1.2. User QSECOFR hanya boleh diakses melalui Console. Status user QSECOFR diubah menjadi DISABLE.

   1.3. Standarisasi Penamaan suatu obyek untuk mempermudah proses identifikasi dan pemeliharaan. Obyek-obyek yang perlu distandarisasi meliputi :

      a. Nama Terminal/display, disesuai-kan dengan segmentasi IP address atau cabang. Misal :

         A050 – KP 192.168.191.50

         B050 – KP 192.168.192.50

         CB50 – Kantor Cibitung, dsb

      b. Nama Printer & Output Queue, menggunakan merek printer + Departemen / divisi / cabang + kode tambahan.Misal :

         HP4050DEP1 : Printer -1 di Departemen Deposit KP

         HP5000BDG1. Printer -1 di cabang Bandung, dsb

III. PROCEDURE

The installation process will be conducted by IBM or IBM business partner. After the installation, Bank will perform the configuration in accordance with Bank's policies and characteristic of application to be used. To ensure the procedure has been executed in accordance with the specified, then use a checklist that contains things that must be fulfilled.

A. Scope

Scope of AS/400 system hardening process are cover :

1. General

   1.1 Connection AS/400 system to/from other applications only allowed for applications which used as production

   1.2 QSECOFR user only can login at Console. To do this, set status of QSECOFR user to DISABLE.

   1.3 Standarization of naming of object to easiliy identification process and maintenance. Naming of objects need to be standarization are :

      a. Terminal/display name, which tailored to IP address segemntation or branches.E.g.:

         A050 – KP 192.168.191.50

         B050 – KP 192.168.192.50

         CB50 – Kantor Cibitung, etc.

      b. Printer & Output Queue name, which used printer brand + Departement/ division / branch + addition code E.g:

         HP4050DEP1:Printer -1 at Head Office Deposit Departement

         HP5000BDG1. Printer -1 at No.1 at Bandung branch, etc.

2. *System Value*

System Value yang berlaku saat ini sesuai pada lampiran – 1.

3. Sistem Operasi dan Perangkat Lunak

Standar perangkat lunak yang digunakan saat ini sesuai pada lampiran – 2.

4. Konfigurasi Jaringan

Konfigurasi jaringan yang digunakan saat ini sesuai pada lampiran – 3.

5. Audit Trail

Pengaturan audit trail yang berlaku saat ini sesuai pada lampiran – 4.

6. Spesifikasi

Spesifikasi mesin yang digunakan saat ini sesuai pada lampiran – 5.

B. Prosedur

1. Prosedur Hardening sistem AS/400:

1.1 Konfigurasi / setting harus dilakukan oleh Security Officer (QSECOFR), dimana dalam penggunaannya akan mengacu pada PEDOMAN PENGGUNAAN USER ID DAN PASSWORD USER ADMINISTRATOR, POWER USER, ROOT DAN QSECOFR.

1.2 Perubahan konfigurasi / setting parameter harus mendapat persetujuan dari Manajemen dan sebelumnya harus dilaporkan ke Direktur in Charge.

1.3 Setiap perubahan konfigurasi / setting parameter harus didokumentasikan sebagai lampiran dari pedoman ini. Dokumentasi harus dapat menjelaskan kondisi yang sedang berjalan, latar belakang / alasan / tujuan perubahan, resiko dan implikasi yang timbul sehubungan dengan perubahan

1.4 Pengecualian prosedur diatas untuk perubahan yang bersifat rutin yang dilakukan oleh Departemen Operasi IT dan perubahan yang bersifat sementara untuk keperluan instalasi perangkat

2. System Value

Current System Value can be seen at Appendix – 1.

3. Operating System and Softwares

Standard softwares to be used for existing condition can be seen at Appendix – 2.

4. Networks Configurations

Network configuration which used for existing condition can be seen at Appendix – 3.

5. Audit Trail

Audit trail setting which used for existing condition can be seen at Appendix – 4.

6. Specifications

The machine specifications currently used can be seen at Appendix - 5.

B. Procedure

1. AS/400 system Hardening procedure:

1.1 Configuration / settings must be made by the Security Officer (QSECOFR) , where the usage will refer to GUIDELINES FOR USE OF USER ID AND PASSWORD USER ADMINISTRATOR , POWER USER , ROOT AND QSECOFR.

1.2 Change configuration / parameter setting must be approved by management and before that must be reported first to the Director in Charge

1.3 Any changes to the configuration / parameter setting must be documented as an appendix of this manual. Documentation must be able to explain the current condition, background / reason / purpose the changes, and the risk and implications arising in connection with the changes

1.4 Exceptions to the above procedure that are routinely performed by IT Operational Departement and temporary changes for installing new devices, such as:

baru, seperti:

- QDATE, QDATETIME dan QTIME : untuk perubahan tanggal dan jam sistem
- QAUTOCFG, QAUTORMT, QAUTVRT : untuk keperluan konfigurasi perangkat baru dan perubahan bersifat sementara.

1.5 Seluruh dokumentasi terkait dengan hardening sistem AS/400 disimpan oleh Departemen Pengembangan TI.

2. Prosedur Instalasi / Update Sistem Operasi & Software pada mesin AS/400 :

2.1 Instalasi dilakukan oleh vendor, dalam hal ini PT. IBM atau Business Partner IBM.

2.2 Instalasi / Update Sistem Software dan atau Sistem Operasi harus mendapat persetujuan Manajemen dan sebelumnya harus dilaporkan ke Director in Charge.

2.3 Sistem Software atau Sistem Operasi yang akan diinstall sudah diperiksa kompatibilitasnya dengan aplikasi yang ada untuk mengurangi resiko kegagalan sistem.

2.4 Setiap instalasi dan update Sistem Software dan atau Sistem Operasi harus didokumentasikan dan disimpan.

3. Prosedur Peyimpanan :

3.1 Seluruh data transaksi dan data aplikasi disimpan dalam suatu media yaitu Tape LTO (Linear Tape Open) dengan kapasitas 2.5 TB.

3.2 Untuk rekam cadang dilakukan oleh Departemen Operasi TI dengan retensi harian,mingguan,bulanan dan tahunan.

3.3 Adapun lokasi penyimpanannya, untuk onsite disimpan di ruang strong room dan untuk offsite disimpan di tempat pihak ke tiga dalam hal ini PT.Iron Mountain sebagi vendor untuk tempat menyimpan data.

- QDATE, QDATETIME dan QTIME : to change system date and time
- QAUTOCFG, QAUTORMT, QAUTVRT : to configure new device and just for temporary changing.

1.5 All documents related hardening AS/400 system kept by IT Developmen Departement.

2. Procedure to install / Update Operating System & System Software on AS/400 machine :

2.1 Installation is done by the vendor, in this case PT. IBM or IBM Business Partner.

2.2 Installation / Update System Software and or Operating System must be approved by the Management and must be reported to the Director in Charge earlier.

2.3 System Software or Operating System that will be installed already checked for compatibility with existing applications so as it can mitigate risk of system failure.

2.4 All the installation and update System Software and or Operating System must be documented and kept.

3. Storage Procedure :

3.1 All transaction data and application data are stored in a media that is LTO Tape (Linear Tape Open) with a capacity of 2.5 TB.

3.2 For backup, the IT Operations Departement is carried out with daily, weekly, monthly and annual retention.

3.3 As for the storage location, for onsite stored in the strong room and for offsite stored at the third party in this case PT. Iron Mountain as a vendor for storing data.

IV. PENUTUP

Pedoman Hardening AS/400 ini diterbitkan dalam 2 (dua) bahasa yaitu Bahasa Indonesia dan Bahasa Inggris dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang menjadi acuan adalah Bahasa Indonesia.

Pedoman Hardening AS/400 ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur tanggal 12 April 2023 dan mencabut Pedoman Hardening AS/400 Edisi 5 April 2021.

Pedoman Hardening AS/400 ini akan dikaji ulang secara berkala paling lambat 2 (dua) tahun sekali atau jika diperlukan sebagai upaya penyempurnaan sesuai dengan perkembangan usaha dan kebutuhan Bank atau perubahan peraturan yang mendasarinya.

IV. CLOSING

Hardening AS/400 Guideline establish in 2 (two) languages, Indonesian Language and English Language, and if there is a difference in the interpretation it will refer to Indonesian Language.

This Hardening AS/400 Guideline is effective as obtain approval by President Director April 12, 2023 and revoke Hardening AS/400 Guidelines, 5th Edition ; April 2021.

This Hardening AS/400 Guideline will be reviewed at latest every 2 (two) years or if needed as an improvement effort following the business development and the need of Bank or following the changes of base regulation.