

# **SKP RESOURCES BHD**

**Bangi Plastics Sdn Bhd (“BPSB”)**

**IT Review for Financial Year Ended 31 March 2021**

## **Management Letter**

- **Plastictenic (M) Sdn. Bhd.**
- **Bangi Plastics**



## **Table of Contents**

1.	Absence of Idle session timeout configuration in SAP ECC6 at application level	3
2.	Absence of Disaster Recovery exercise	5
3.	Improvement of SAP User ID Management	6
	APPENDICES	7

## 1. Absence of Idle session timeout configuration in SAP ECC6 at application level

### Observations

We noted that SKP Resources Berhad has an Information Security Password Policy, IS-PS02, which provides a guideline of password configuration under Section 4.2 Guidelines, Sub-section A. General Password Construction Guidelines. Below is the configuration password guideline:

<b>Password Policy</b>	<b>Recommended Settings</b>
Password History	3 – 5 passwords remembered
Maximum Password Age	90 days
Minimum Password Age	1 days
Minimum Password Length	8 characters
Minimum Password Symbol	1
Minimum Password Number	1
Password Complexity	Enabled
<b>Account Lockout Policy</b>	<b>Recommended Settings</b>
Account Lock Duration	0 minutes (Until administrator unlocks)
Account Lock Threshold	3 – 5 invalid logon attempts
Reset Account Lockout Counter After	0 minutes (Until administrator unlocks)
<b>Time Out Policy</b>	<b>Recommended Settings</b>
Active Session Limit	2 Hours
Idle Session Limit	20 minutes

However, during our course of review, we noted that the idle session timeout for SAP EEC6 at application level is not configured as per policy. Below is the table summary:

<b>Password Configuration</b>	<b>Current configuration in system</b>	<b>SKP Policy Guideline</b>
Idle Session Limit	<b>0</b>	<b>20 minutes</b>

Please refer Appendix A

### Risks Implications

The absence of the idle session timeout will allow unauthorized personnel to access the system information/data or perform any fraudulent activities under the impersonation of authorized personnel if the system user account left unattended. This may lead to unauthorized system access.

## Recommendations

We recommend that Management:

- a) To comply with the current SKP Resources Berhad's Information Security Password Policy and configure the idle session timeout in SAP ECC6 at application level to 20 minutes accordingly.

## Management's Comments

Our SAP actually is already configured the idea session which the evident can find in Transaction code RZ11 under rdisp/gui\_auto\_logout. However, no idea why the 1<sup>st</sup> RMPARAM screen shot is not showing the right configure system.

The screenshot shows the SAP 'Display Profile Parameter Attributes' window for the parameter 'rdisp/gui\_auto\_logout'. The window title is 'PRD (1) 777' and the browser address bar shows 'PRD (1) 777'. The parameter name is 'rdisp/gui\_auto\_logout'. The short description is 'Maximum Time of no Input at the GUI'. The application area is 'Dispatcher and Task Handler'. The parameter type is 'Character String'. The changes allowed are 'Change permitted'. The valid for operating systems is 'All operating systems'. The dynam. switchable checkbox is checked. The same on all servers checkbox is unchecked. The default value is '0', the profile value is '1800', and the current value is '1800'. The window also shows a navigation bar with 'Documentation', 'Change Value', 'Cancel', and 'More' options. The taskbar at the bottom shows various application icons and the system clock indicating 1:36 PM on 11/5/2021.

Parameter Name	Value
rdisp/gui_auto_logout	1800

Attribute	Value
Short Description (EngL)	Maximum Time of no Input at the GUI
Application Area	Dispatcher and Task Handler
Parameter Type	Character String
Changes allowed	Change permitted
Valid for Operating Sys.	All operating systems
Dynam. switchable	<input checked="" type="checkbox"/>
Same on all servers	<input type="checkbox"/>
Default Value	0
Profile Value	1800
Current Value	1800

**Action Party:**

After checking and the RSPARAM now is already can show in the configuration report

Parameter Name	User-Defined Value	System Default Value	System Default Value(Unsubstituted Form)
rdisp/dplcomlib_path	G:\usr\sap\PRD\DVEBMGS00\exe\dplcomlib.dll	G:\usr\sap\PRD\SYSEXE\run\dplcomlib.dll	(Default)
rdisp/dynamic_wp_check		TRUE	TRUE
rdisp/early_snc_handshake		0	0
rdisp/elem_per_queue		2000	2000
rdisp/enq_serv_reset		1	1
rdisp/enqname	ptsbprd00_PRD_00		
rdisp/ext_timer_stop_delay		300	300
rdisp/fileTableCheck		off	off
rdisp/frfc_fallback		on	on
rdisp/gui_auto_logout	1800	0	0
rdisp/gui_cleanup_delay		0	0
rdisp/http_check		1	1
rdisp/http_min_wait_dia_wp		1	1
rdisp/icm_startup_args			
rdisp/invalidate_memory		00	00
rdisp/j2ee_error		10	10
rdisp/j2ee_libpath	G:\usr\sap\PRD\DVEBMGS00\j2ee\os_libs	G:\usr\sap\PRD\D00\j2ee\os_libs	\$(DIR_INSTANCE)\\$(DIR_SEP)j2ee\\$(DIR_SEP)os_libs
rdisp/j2ee_op		0	0
rdisp/j2ee_profile	\ptsbprd00\sapmnt\PRD\SYSPROFILE\PRD_DVEBMGS00_ptsbprd00	\ptsbprd00\sapmnt\PRD\SYSPROFILE\PRD_DVEBMGS00_ptsbprd00	\$(SAPPROFILE_IN_EFFECT)
rdisp/j2ee_start		0	0
rdisp/j2ee_start_control		1	1
rdisp/j2ee_start_lazy		0	0
rdisp/j2ee_timeout		60	60

**Target Date of Implementation:**  
Completed

## **2. Absence of Disaster Recovery exercise**

### **Observations**

We noted that SKP Resources Berhad has procedure called Service Continuity and Availability Management, SCA-SP01 which gives guideline on business continuity plan to ensure the service continuity and availability management in place to support the business requirement. In this policy, under section 3.1.2 Description, sub-section a) Disaster Recovery Test Procedures, we noted the following statement: -

- “IT Department schedules one disaster recovery test per year with sufficient time to test the operating system and customer Disaster Recovery Plan checklist.”

However, during our review, we noted that there is an absence of a Disaster Recovery exercise being performed for the financial period.

### **Risks Implications**

Without a DR testing being performed, the management is unable to gain comfort that the company is able to recover system and data as and when required and its critical systems in the event of a disaster within the Recovery Time Objective (RTO) defined by business users.

### **Recommendations**

We recommend that Management:

- a) To comply to Service Continuity and Availability Management procedure to perform the disaster recovery exercise once a year.
- b) Results of the DR tests, including issues encountered and corresponding resolution actions taken should be documented and retained for future reference.

### **Management’s Comments**

Last year, 2020 has been a challenging year and a lot unexpected issue. However, we still plan to have DR test but there is no report have been documented.

### **Action Party:**

Start 2021, we put the DR testing under our SAP Server monthly maintenance activity in Q4 November. Onward every year will continue this activity in Q4

### **Target Date of Implementation:**

Q4 2021

### 3. Improvement of SAP User ID management

#### Observations

During our review on user access management, we understand there are a total of forty-seven (47) SAP user IDs in the system. However, we identified there are forty-one (41) user IDs out of the total forty-seven (47) were tagged under a generic SAP User ID.

The SAP user ID in SKP Resource Berhad environment is assigned under the generic SAP ID name instead of a unique SAP ID tied to the users. A predefined generic SAP user ID is created whereby upon the ID availability, it will be assigned to the new user/new hire that commensurate to their job role.

All the information of the users assigned to respective SAP ID is tracked and maintained in a spreadsheet which consists of the following information:

- SAP generic user ID
- Key user's name
- Key user's designation
- Status
- Last Modified
- Remarks

When there is a change in user/personnel, the IT department will reassign the generic SAP user ID to the new user without deleting or recreating the user profile. Subsequently, the IT department will update the tracker with the latest information of the user for monitoring purposes.

Please refer to **Appendix B** for the sample of the manual tracker of SAP key user IDs.

#### Risks Implications

- i. Maintaining the SAP user ID manually via spreadsheet may have the tendency to overlook the list or update the list with an error. This may inherent risk of accountability of the SAP ID usage in the system.
- ii. Usage of general SAP user ID with the change of users' overtime may compromise the usage of system audit trail to identify the respective individual user accounts associated with certain events/activity performed. By using the generic SAP ID, there may be a risk of not detecting the correct individual who has performed certain activity but relying on the identity of the ID via the manually maintained spreadsheet which may not be reliable.
- iii. As the IT department is the custodian of manual tracker of the SAP user ID, any unauthorized activity performed by the SAP user ID may fall under the responsibilities of the IT department to evaluate and identify the correct ID. This may involve an accountability issue or risk in determining and identifying the correct source if it is only based on a single source of data (the manual spreadsheet).

## **Recommendations**

We recommend that Management:

- a. To restructure the SAP user IDs in the SAP system by creating the SAP user IDs based on the current key user's unique identifications (E.G name of the key user, surname of the key user, employee number, and etc).

## **Management's Comments**

Understand that using user's name as an id keyword is better. But base on the record from pass years, rate for change user is very high and this is because of user resigned from their position. Therefore, we not prefer to put user name as ID key word.

## **Action Party:**

This ID culture is adopted since the first day SAP implementation until now so it needs to take time to have this improvement. We will restructure the SAP ID to this improvement from time to time

## **Target Date of Implementation:**

In year 2024

## Appendix A

rdisp/delayed_call_interval		60		60	Time cycle for invoke of delayed functions
rdisp/delete_ddlog		on		on	Cyclic Refresh of Table DDLOG
rdisp/dev_loop		OFF		OFF	
rdisp/dp_check_logoff_flags		0		0	
rdisp/dplcomlib_path	G:\usr\sap	G:\usr\sap\PRD\SYS\exe\run\dp		(Default)	
rdisp/dynamic_wp_check		TRUE		TRUE	
rdisp/early_snc_handshake		0		0	
rdisp/elem_per_queue		2000		2000	Number of Requests per Work Process
rdisp/enq_serv_reset		1		1	
rdisp/enqname	ptsbprd00	PRD_00			Name of the Enqueue Server
rdisp/ext_timer_stop_delay		300		300	
rdisp/fileTableCheck		off		off	
rdisp/frfc_fallback		on		on	
rdisp/gui_auto_logout		0		0	Maximum Time of no Input at the GUI
rdisp/gui_cleanup_delay		0		0	
rdisp/http_check		1		1	Enable dispatcher check for HTTP/SMTP req
rdisp/http_min_wait_dia_wp		1		1	Number of waiting dialog work processes
rdisp/icm_startup_args					
rdisp/invalidate_memory		0		0	
rdisp/j2ee_error		10		10	Number of start errors before deactivating r
rdisp/j2ee_libpath	G:\usr\sap	G:\usr\sap\PRD\D00\j2ee\os_lit		\$(DIR_INSTANCE)\\$(DIR_SEP)j2ee	j2ee path for shared library
rdisp/j2ee_op		0		0	internal opcode for monitoring
rdisp/j2ee_profile	\\ptsbprdC	\\ptsbprd00\sapmnt\PRD\SYS\pr		\$(SAPPROFILE_IN_EFFECT)	alternative name for SAP J2EE Engine profile
rdisp/j2ee_start		0		0	Enable start of J2EE engine
rdisp/j2ee_start_control		1		1	control start J2EE engine
rdisp/j2ee_start_lazy		0		0	start J2EE engine after ABAP initialastion
rdisp/j2ee_timeout		60		60	Reconnect timeout for J2EE Engine

## Appendix B

No.	User Logon ID	Key User	Designation	Status	Last Modified	Remark
1	IT01	Kelvin Tan	Executive	Active	NA	Admin
2	B_ENG01	Tan Mi Ping	Officer	Active	NA	
3	B_ENG02	Low Bee Gee	Senior Executive	Active	NA	
4	B_FIN01	Lee Yoke Lan	Manager	Active	NA	
5	B_FIN02	Wan Voon Tse	Officer	Active	NA	
6	B_FIN03	Lai Choi Lih (Cheryl)	Officer	Active	NA	
7	B_PLAN01	Rosna Rina Binti Yahya	Officer	Active	NA	
8	B_PLAN02	Wong Pei Shan (Fenny)	Officer	Active	NA	
9	B_PLAN03	Yap Li Lee	Senior Executive	Active	NA	Replace Ooi Chee Seng
10	B_PROD02	Packialetchumy A/P Thangiah	Executive	Active	NA	
11	B_PROD03	Wayidah Binti Abdul Kadar	Senior Executive	Active	NA	
12	B_PURCH01	Yong Yuen Thai (Yvonne)	Assistant Manager	Active	NA	
13	B_PURCH02	Liow Shi Yi	Officer	Active	NA	
14	B_QA02	Sarajini A/P Chinniah	Assistant Manager	Active	NA	
15	B_SALES01	Goo Min Wah (Rachel)	Executive	Active	NA	
16	B_TCD02	Jayanthi A/P Palany	Officer	Active	NA	
17	B_WHSE01	Mohd Saberi Bin Muhd Zain	Executive	Active	NA	
18	B_WHSE02	Maisarah Binti Said	Officer	Active	NA	
19	N_ENG01	Chandra Devi A/P Chinniah	Officer	Active	NA	
20	N_ENG02	Lai Jiun Siong	Assistant Manager	Active	NA	
21	N_FIN01	Chiak Yuet Chan	Manager	Active	NA	
22	N_FIN02	Norhaslina Bt Mohd Hanafi	Executive	Active	NA	
23	N_FIN03	Wong Pik Mei	Executive	Active	NA	
24	N_PLAN01	Tang Wen Yin (Agnes)	Planner	Active	NA	
25	N_PLAN02	Gan Mei Wann	Officer	Active	NA	
26	N_PLAN03	Lee Wei Hong	Operation Manager	Active	NA	
27	N_PROD01	Nita	Clerk	Active	NA	