TEMENOS
The Banking Software Company

PRODUCT

Secure Coding Standards for T24

Amendment History

Version Number	Date	Author/Changed by	Description of Changes Made
0.1			Initial Draft
0.2	18-Oct-12	Smitha Nair	Formatting done for the existing document
1.0	19-Oct-12	EPG Subgroup	Baselined for publishing.

Contents

1. Introduction

T24 Programming standards are available in Knowledge base under path **http://knowledgebase.temenosgroup.com/t24/Pages/Development%20Process.aspx >** Development Process guides > User guides section .

It should be used for complete understanding of basic programming standards.

Scope of this document is to further explain the Secure Coding Standards applicable for development in T24

2. Fundamentals

2.1 Basics

- Avoid using common variables to pass as parameters in subroutines
- Avoid using transaction, boundary related core common variables – except in core programs where it is specifically required. Any update to core COB files – eg JOB.LIST, its related locking updates etc should be avoided.
- Ensure that code does not alter global common variables like TODAY, ID.COMPANY, R.COMPANY, R.DATES etc within application code. Only the components/subroutines that own these common variables could change them. For example ID.COMPANY could be changed by LOAD.COMPANY.
- Ensure that named common variables are only assigned in the appropriate routines. For example named commons used in batch – should only be assigned in the load routine. The record /Select routine should only use them not alter values in them unless functionality demands it
- When common variables need to be used in programs ensure that they are reset after they are expected to be out of scope.

2.2 Information leakage

- Ensure not to log highly sensitive information where possible. Logging should only use T24 logger framework
- System memory variables should not be used to log any sensitive information as it can be misused /monitored by others

2.3 Access Control

- EB.CALL.API should be used where an API request to be done. This will ensure that core common variables are preserved so that it cannot be tampered by API's
- DAS should be used for selecting records from applications. No Direct SELECT should be used. This will have a control on SELECT's performed on applications are permitted by application owner.

2.4 Insecure Storage

- Data should be in database files and not directly directory structure of T24 – Eg writing directly to run directory should be avoided.