1 DBMS cPP SECURITY PROBLEM DEFINITION

In this document the security problem definition (SPD) for a DBMS is described. The formal description of the SPD is presented in terms of the identified threats, policies, and assumptions that will be used to identify the specific security requirements addressed by this cPP.

1.1 Assets and Threat Agents

The threats given in Section 1.2 refer to various threat agents and assets. The term "threat agent" is defined in CC Part 1.

The assets, mentioned in Table 1 below, are either defined in CC Part 1, or in the glossary which will be provided in the Appendix of the cPP document.

The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms "public objects" and "TOE resources" are given in the glossary which will be provided in the Appendix of the cPP document.

1.2 Threats

The following threats are identified and addressed by the TOE and should be read in conjunction with the threat rationale.

Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by the organization, law or regulation.

Table 1: Threats Applicable to the TOE

Threat	Definition
T.ACCESS_TSFDATA	A user or a process may read or modify TSF data using functions of the TOE without being identified, authenticated and authorized.
T.ACCESS_TSFFUNC	A user or a process may use, manage or modify the TSF, bypassing the protection mechanisms of the TSF.
T.IA_USER	A user who has not successfully completed identification and authentication may gain unauthorized access to user data or TOE resources beyond public objects.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.UNAUTHORIZED_ACCESS	An authenticated user or a process, in conflict with the TOE security policy, may gain unauthorized access to user data.

1.3 Organizational Security Policies

The following organizational security policies are addressed by cPP-conformant TOEs:

Table 2: Policies Applicable to the TOE

Policy	Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible while supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly and are permitted by the organization to access user data.

25 ## 1.4 Assumptions

26 This section contains assumptions regarding the IT environment in which the TOE will reside.

27 **Table 3: Assumptions Applicable to the TOE Environment**

Assumption	Definition
Physical aspects	
A.PHYSICAL	The operational environment is assumed to provide the TOE with appropriate physical protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.
A.MANAGE	The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Authorized users are sufficiently trained to accomplish a task or a group of tasks within a secure IT environment by exercising control over their user data.
Procedural aspects	
A.NO_GENERAL_ PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_ MGT	All remote IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically and/or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

28