Module 5 -Computer Systems (2021-22)
Project

UNIVERSITY OF TWENTE.

Security by Design Checklist
(Requirement Analysis Phase 1)

Team ID:	**Team Members:**
Project Name:	**Mentor(s):**

Steps to be performed:

i) You should select a minimum of one security mechanism from each of the security requirements from authentication and authorization both (auditing is not included here).

ii) The auditing requirements should be considered as suggested in the table according to your application. Other than the normal check on protecting log files, backup files, etc, you should also think about the GDPR obligations, software licensing, etc. in line with your application.

iii) The given security mechanisms are for your inspiration. You can select other mechanisms also according to the requirement of your application. For example: If you select "authentication" as one of the security requirements, the mechanism can be logging/password checking, biometric, OAuth, etc. The same is applicable for authorization and auditing.

iv) Justify the reason to select a particular mechanism for the requirements in the given column 'C'.

v) Write supplement requirement(s) in the form of a user story ar Abuse case for the application (refer to the example given on the table, column 'D'). (The supplement requirements should be according to the goals and non-functional requirement (s) identified for your application.)

vi) Write the possible risks involved for the supplement requirements (refer to the example given in the table, column 'E').

vii) Write the resources/mechanisms/tools to avoid/mitigate those risks for security controls (refer to the example of the column heading "Appropriate Security Control" (column 'F')).

viii) This document must be reviewed with the team members and approved by your mentor(s)/TAs.

ix) Put tickmark in the last column for all verified items.

x) This document should be appended to the Software Requirement Specification (SRS) document.

Follow these 5 points for each of the Security Mechanisms and write them under Appropriate Security Controls

i) Supplement security requirements to avoid risk.

ii) Write the requirement of the resources to mitigate such risks. For example: The type of Authentication software, security tokens, password management software, etc.

iii) Devise a plan/method (tentative) to work on the identified risks.

iv) Review the documentation within your team.

v) Approve the document by your mentor.

Security Policy	Confidentiality, Integrity, and Availability					
Security Requirements	**Security mechanisms (List down for your application)**	**Remarks on why you considered these requirements? (in a brief)**	**Supplement requirements for your application (user story/Abuse case)**	**Risk identification/Threat Assessment (at least one risk identification/abuse case)**	**Appropriate Security Controls**	**Tick ✔ if you have applied the given security controls as suggested in the left column**
Authentication	**For example:** Checking password	**For Example:** for granting access to multiple users and for users to have their individual profiles, we need to authenticate their username with a password. A more sophisticated authentication is not required. (Justify Why)	**Example Goal:** The system verifies that there are no default passwords used by the application or any of its components. Requirement: To access the application, one should require authentication. User story: "As a user, I can enter my user name and passwords to access the application." Abuse Case: As an attacker, I can enter the default passwords to access the application.	**Example Risk identication:** i) The length of the passwords is less than 1023 characters., ii) The password is not very strong., iii) You enter a wrong password more than 3 times, etc.	Follow the 5 points mentioned above.	
	Examples: Biometric, Account security via Two factor authentication/Multi Factor Authentication, Smartphone communication (registered phone number), OAuth, Proof of User's physical presence for authentication (https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication), Proximity based authentication, etc.				Follow the 5 points mentioned above.	
Authorization	Access control policies-User based, role-based, etc.				Follow the 5 points mentioned above.	
Audit	Protection of Log files,				Follow the 5 points mentioned above.	
	Backup files,				Follow the 5 points mentioned above.	
	Temporary files, software and database licenses (Legal aspect), processing of personal identifiable information on the devices (Legal aspect/GDPR policies), etc.				Follow the 5 points mentioned above.	

Team members' reviewed: (Member 1, Yes), (Member 2, Yes),…

Mentor(s) reviewed and verfied: (Mentor 1, Yes), (Mentor 2, Yes), …

Prepared by:

Dipti K. Sarmah (Project Coordinator)