ICTWEB513 - Q5.2

# Table of contents

# 

[**Table of contents**](#_heading=h.30j0zll) **2**

[Authentication](#_heading=h.loiitj9w0ncu) **3**

[**Authorisation**](#_heading=h.walbbus0ikah) **4**

[**Availability**](#_heading=h.6h04l9fmuk87) **5**

[**Confidentiality**](#_heading=h.asrg48xbz1be) **6**

[**Integrity**](#_heading=h.2vgxnlss2eg3) **7**

# 

# Authentication

The website relies only on names being entered; the method used is extremely unsecure. At the very least, we can implement a password system to increase the security of the site.

# 

# Authorisation

After the user is authenticated and logged in, we store the data into the session and only after this, the user can see the private sections or pages of the site. Once the user logs out or the session is cleared, there’s no more access to those areas. We have 3 different authorisation roles: admin, staff, customer which has different dashboards according to your role.

# 

# Availability

As a local system, it is available to the time the MAMP server is up and running, however,

it is not a concern for now.

Moreover, nowadays, high availability is easily achievable by using cloud computing services to host the system.

# 

# Confidentiality

All the data is stored as plain text/numbers, but there’s no confidential information except for names maybe.

# 

# Integrity

There are no integrity validations, sanitizations and consistency checks. Not even at the database level, we didn’t implement relational integrity, fields types, etc, which could add a bit of consistency to the data.