List of Security Standards Our Website must meet

1. TLS Encryption Standards; This would not apply to us just yet if we are not necessarily hosting the website, however it is very important of us to note that we should make use of TLS 1.2 or above for a more secure data transmission. To get this covered, we would look at implementing HTTPS with TLS to protect data on transit.
2. Access Control Standards (NIST 800-53); We must make sure that access to the data on the page is controlled
3. enetration Testing and Vulnerability Assessments: As it states, we must carry out a vulnerability assessment and test our website security.
4. ISO/IEC 22301: Business Continuity Management System; In the likelihood that the website goes down for a bit, what are our backup plans, especially if the site becomes a critical support for student.
5. ISO/IEC 29100: Privacy Framework; In the way this applies to us, we must ensure that none of the users personal data is at risk since we are not collecting personal data.
6. NHS Data Security and Protection Toolkit (DSPT); This would apply to us as we are gonna be dealing with mental health, therefore we must meet the NHS standards for protecting health data, even though the website is not part of the NHS networks.
7. General Data Protection Regulation (GDPR) Compliance; This does not generally apply to us as we won’t actively be collecting personal identifiable information (PII), but we have chosen to note this still as an important guideline.

After accessing our website, below are security standards we can implement.  
  
1. Content Security Policy (CSP)

As of now, none of our files currently implements a Content Security Policy. To protect against XSS and data injection attacks, we should consider including a CSP in the <head> section of our HTML files. The sources from which scripts, styles, and graphics can load are limited by this policy. While excluding unauthorised sources, a CSP setup would permits scripts and styles from the designated external sources. It is a strong form of security for us.

2 I have seen that we don’t meet the HTTPS Requirements, even if we don’t host the actual website just yet, it could be a good security practice to apply these protocols to our code. We can use the Strict Transport Security header in server configuration to enforce this.

I have also noticed a few errors in the code, but I want to believe that’s not everything as we don’t yet have a css nor JS code in their respective files.