**Security Design**

**Technology Based Risks and Design Choices**

SQL Injection

Any system that has a user interfacing with a SQL database in any way (although in particular through forms) can potentially be vulnerable to SQL injection attacks from malicious sources (or even accidentally). Although one of the most common types of attacks, SQL injection is very easily mitigated using rigorous input sanitisation and strictly limiting user database access to predefined queries hardcoded into the site backend itself.

Connection Security

These days it is assumed that a site will support HTTPS connections to and from its servers, ours will be no different with SSL used to secure communications between the server and the end user to ensure nobody in between listens in on anything they shouldn’t.

Direct Linking to files

We will not allow direct linking to media files on our servers via external links, there are a few simple reasons for this. First and foremost being rights management for our contributing users, depending on the privacy settings chosen for a given uploaded media the user may not desire that it be publically available, or if they do want it publically available, they may not wish for the source file to be \*freely\* available. Conversely, allowing external sources to link directly to our files could allow our files to be embedded in external sites, which would result in a loss of traffic, but an increase in data usage by the server, which is understandably something we want to avoid.

Backups

This should go without saying but frequent backups of all systems will be made automatically. Full backups on a weekly basis with incremental backups performed daily. Thus in the event of any catastrophic disaster, the site and its data can be saved and restored in a timely manner.

**User Level Security**

Access Controls

As with any web service featuring social aspects, our site will implement the ability for users to control the visibility of various aspects of their content. Aspects of their profile can be set to public or private, with public set details visible to any site user while private details are visible only to a select few on the site (Potentially collaborators or through a ‘friends’ system. The exact details of the implementation are still being hammered out). Media uploads will include an ‘unlisted’ option, where the media is not listed in search results or on the site front page but can be linked to and publically accessed.

User Harassment

Because users have the ability to comment on content on the site, there will invariably be a few who choose to abuse this system, to this end, the owner of a piece of content (media, profile, etc) can opt to ‘block’ a user. This will prevent the blocked user from interacting with the blocking user in any way, effectively making it as if the blocking user does not exist from the perspective of the blocked user. The blocking user may still be able to view content belonging to the blocked user, but will be unable to comment or interact with it.

TOS Violations or Rights Abuse

If a user suspects that another user has in some way breached the site TOS (such as uploading inappropriate content or claiming content they do not actually own), the user is able to issue a ‘report’ that will be investigated by the site admins for legitimacy. If the report is found to be legitimate, the administrators will decide on an appropriate response, whether that be taking down the offending content or banning the user outright. If a user repeatedly files fraudulent reports, they will be punished.

**Risk Response**

System Breach

In the unlikely (but always possible in today’s world) even of a system breach that leaves any user data on the site exposed, all user passwords will be reset (requiring a password change on next login), any potentially exposed encryption keys will be discarded and updated, and all users will be notified that a breach has occurred and the steps taken to mitigate risks to their personal data. When such a breach occurs, methods will be investigated and implemented to close the security hole that allowed the unauthorised access to occur.

Database Damage

If somehow the database manages to become damaged (through malicious intent or otherwise) there are several courses of action we can take. In the case of smaller issues (such as corrupted transactions) a simple database rollback can be done to undo the damage, while in more severe cases, we can resort to restoring the system from a previous backup, while this would result in some data loss, under certain circumstances it may be unavoidable.