# CS632 – IT PROJECT MANAGEMENT

**RISK MANAGEMENT PLAN – STUDENT CONNECT WEBSITE (GROUP 6)**

1. **PROJECT SUMMARY:**

* To create a website that allows students from different universities to connect and collaborate.
* To provide a platform for developing strong social ties among students.
* To improve student’s skills in communication, teamwork, and problem-solving.
* To facilitate exploration and enhancement of students’ knowledge in a broader perspective.
* To develop features for networking, studying, building projects, and exchanging ideas.
* To promote active engagement and learning among students through online collaboration

1. **RISK IDENTIFICATION:**

|  |  |  |
| --- | --- | --- |
| **Risk Id** | **Risk** | **Description** |
| 1 | Technical Failure | A risk that the Student Connect website may experience technical issues, such as bugs, glitches, or errors that could lead to an interruption in service or loss of functionality. |
| 2 | Security Breach | A risk that unauthorized individuals or hackers could gain access to sensitive information, such as user data or financial information, which could lead to identity theft or financial losses. |
| 3 | Intellectual Property Infringement | A risk that Student Connect may unknowingly violate the intellectual property rights of others by using copyrighted material, trademarks, or patents without permission. |
| 4 | Inappropriate User-Generated Content | A risk that users may post inappropriate or offensive content on the website, such as hate speech, harassment, or pornography, which could damage the website's reputation or lead to legal consequences. |
| 5 | Server Downtime | A risk that the website's servers may experience downtime or become unavailable due to technical issues, maintenance, or other reasons, which could lead to a loss of service or revenue. |
| 6 | Lack of Traffic | A risk that the website may not attract enough visitors or users to sustain its operations or generate revenue, which could lead to financial losses or the need to shut down the website. |
| 7 | Loss of Data | A risk that the website may lose important user data, such as login information, contact information, or user preferences, due to technical issues, hacking, or other reasons, which could damage the website's reputation or lead to legal consequences. |
| 8 | Legal Issues | A risk that the website may face legal challenges, such as copyright infringement, defamation, or privacy violations, which could lead to lawsuits or fines. |
| 9 | Poor User Experience | A risk that the website may provide a poor user experience, such as slow loading times, difficult navigation, or confusing layout, which could lead to user frustration, decreased engagement, or loss of revenue. |
| 10 | Content Duplication | A risk that the website may inadvertently duplicate content from other sources, which could lead to accusations of plagiarism or copyright infringement. |
| 11 | Poor Performance | A risk that the website may perform poorly in terms of speed, reliability, or functionality, which could lead to user dissatisfaction, decreased engagement, or loss of revenue. |
| 12 | Inadequate Funding | A risk that the website may not receive enough funding to sustain its operations, which could lead to financial losses or the need to shut down the website. |
| 13 | User Abandonment | A risk that users may abandon the website due to poor user experience, lack of features, or other reasons, which could lead to decreased engagement or loss of revenue. |

1. **RANKING THE BAD RISKS (THREATS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **1🡨----------------------------------------------------------------------------- 0**  **Probability** | **High** | |  |  | **4,9,11,13** | **6** |
| **Medium** | |  |  | **1** | **2,5** |
| **Low** | |  |  | **10** | **3,7,8,12** |
|  | |  | **Low** | **Medium** | **High** |
|  | | 1. **Impact -----------------------------------------------------------------------------**🡪 **1** | | | | |

1. **QUANTIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Id** | **Risk** | **Probability of Occurrence** | **Impact** |
| 1 | Lack of Traffic | High | High |
| 2 | User Abandonment | High | Medium |
| 3 | Poor Performance | High | Medium |
| 4 | Poor User Experience | High | Medium |
| 5 | Inappropriate User-Generated Content | High | Medium |
| 6 | Server Downtime | Medium | High |
| 7 | Security Breach | Medium | High |
| 8 | Technical Failure | Medium | Medium |
| 9 | Inadequate Funding | Low | High |
| 10 | Legal Issues | Low | High |
| 11 | Loss of Data | Low | High |
| 12 | Intellectual Property Infringement | Low | High |
| 13 | Content Duplication | Low | Medium |

1. **POSSIBLE RISK RESPONSE (MITIGATION STEPS)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk Name** | **Probability**  **H/M/L** | **Impact (use H/M/L)** | | | | **Score**  **H/M/L** | **Explain Risk Response (Indicate – Transfer/Mitigate/Prevent/Ignore).** |
| Scope | Quality | Schedule | Cost |
| Lack of Traffic | H | H | M | H | M | H | Mitigate |
| User Abandonment | H | M | M | H | M | M | Mitigate |
| Poor Performance | H | M | H | H | H | H | Mitigate |
| Poor User Experience | H | M | H | H | H | H | Mitigate |
| Inappropriate User-Generated Content | H | M | H | M | L | M | Prevent |
| Server Downtime | M | H | H | M | H | H | Mitigate |
| Security Breach | M | H | H | M | H | H | Prevent |
| Technical Failure | M | M | M | H | H | M | Mitigate |
| Inadequate Funding | L | H | M | H | H | H | Transfer |
| Legal Issues | L | H | H | H | H | H | Transfer |
| Loss of Data | L | H | H | H | H | H | Prevent |
| Intellectual Property Infringement | L | H | H | H | H | H | Prevent |
| Content Duplication | L | M | M | M | L | M | Ignore |

Top of Form

**6. RISK CONTINGENCY PLAN**

|  |  |  |
| --- | --- | --- |
| **Risk Name** | **Rating after Risk Response** | **Contingency Steps should the risk materialize** |
| Lack of Traffic | H | Increase marketing efforts and advertising campaigns to attract more traffic to the platform |
| User Abandonment | H | Conduct user surveys to identify pain points and implement changes to improve user experience |
| Poor Performance | H | Invest in performance testing and optimization to improve the platform's speed and responsiveness |
| Poor User Experience | H | Conduct user experience testing and make necessary improvements to the platform's design and functionality |
| Inappropriate User-Generated Content | H | Implement content moderation tools and policies to prevent inappropriate content from being published |
| Server Downtime | M | Have backup servers in place and regularly test disaster recovery protocols to minimize downtime |
| Security Breach | M | Implement robust security measures such as two-factor authentication, encryption, and regular security audits |
| Technical Failure | M | Have a support team in place to quickly address technical issues and implement redundancy measures for critical systems |
| Inadequate Funding | L | Secure additional funding through investors, crowdfunding, or other means to ensure continued operations |
| Legal Issues | L | Consult with legal experts to ensure compliance with laws and regulations, and be prepared to take legal action if necessary |
| Loss of Data | L | Implement regular data backups and disaster recovery protocols to minimize data loss in the event of an outage or failure |
| Intellectual Property Infringement | L | Monitor and protect the platform's intellectual property, and be prepared to take legal action against infringing parties |
| Content Duplication | L | To avoid content duplication, focus on creating unique and high-quality content. Use plagiarism checker tools to ensure that your content is original. |

1. **TRIGGER IDENTIFICATION:**

* **Content Duplication** - Plagiarism, copying content without permission, using duplicate content across different pages or sites.
* **Intellectual Property Infringement** - Using copyrighted materials without permission, trademark infringement, stealing trade secrets, patent infringement.
* **Loss of Data** - Data breaches, hacking, theft, system failure, accidental deletion or corruption, natural disasters, power outages
* **Legal Issues** - Violating regulations, non-compliance with laws or policies, facing lawsuits or legal action, contract disputes.
* **Inadequate Funding** - Insufficient budget, overspending, lack of investors or supporters, limited financial resources.
* **Technical Failure** - Hardware or software malfunctions, bugs, errors, compatibility issues, system crashes, network failures
* **Security Breach** - Cyberattacks, unauthorized access, data theft, hacking, phishing, social engineering, malware, ransomware.
* **Server Downtime** - Maintenance or upgrades, power outages, server overload, network issues, DDOS attacks, hardware failure
* **Inappropriate User-Generated Content** - Offensive or harmful comments or posts, hate speech, spam, inappropriate images or videos.
* **Poor User Experience** - Slow loading times, difficult navigation, unclear or confusing design, broken links, poor accessibility, lack of mobile optimization
* **Poor Performance** - Low search engine rankings, slow site speed, high bounce rates, low conversion rates, poor engagement metrics
* **User Abandonment** - Lack of user engagement, low retention rates, high churn, poor user satisfaction, ineffective marketing or promotion
* **Lack of Traffic** - Poor search engine optimization, low social media visibility, weak marketing efforts, lack of audience targeting, ineffective content promotion

1. **RISK CONTROL:**

* **Content Duplication:** Regularly scan the website's content using plagiarism detection tools. Encourage original content creation and educate content creators on the consequences of content duplication.
* **Intellectual Property Infringement:** Implement procedures to verify the ownership of all content and images used on the website. Monitor the website for unauthorized use of copyrighted material and respond to any infringement claims promptly.
* **Loss of Data:** Regularly back up all data, implement robust security measures to protect against data breaches, and have a disaster recovery plan in place.
* **Legal Issues:** Stay up-to-date with relevant laws and regulations, implement terms and conditions of use, and seek legal advice when necessary.
* **Inadequate Funding:** Monitor the budget and expenses closely, prioritize spending on critical functions, and seek additional funding sources when necessary.
* **Technical Failure:** Regularly test and maintain all technical systems, implement redundancy and backup solutions, and have a plan in place to address technical failures quickly.
* **Security Breach:** Implement robust security measures, monitor the website for potential threats, and have a response plan in place to address security breaches quickly.
* **Server Downtime:** Regularly monitor server performance, implement redundancy and backup solutions, and have a plan in place to address server downtime quickly.
* **Inappropriate User-Generated Content:** Implement strict content guidelines, monitor user-generated content closely, and have a response plan in place to address inappropriate content quickly.
* **Poor User Experience:** Regularly monitor user feedback and user experience metrics, implement user-centered design principles, and continually improve the website's usability and functionality.
* **Poor Performance:** Regularly monitor website performance metrics, implement performance optimization techniques, and have a plan in place to address poor performance quickly.
* **User Abandonment:** Regularly monitor user behavior metrics, implement user retention strategies, and continually improve the website's value proposition.
* **Lack of Traffic:** Implement effective SEO and marketing strategies, monitor website traffic metrics, and continually improve the website's visibility and reach.

1. **SUMMARY OF ACTION PLANS FOR THE RISKS WE CHOSE TO MITIGATE**

* **Content Duplication:**
  + Task: Conduct regular checks for duplicated content using plagiarism checker tools.
  + Duration/Effort estimate: Monthly check taking about 4 hours per month.
  + Responsible party: Content Manager
* **Intellectual Property Infringement:**
  + Task: Monitor the website content for any infringement of intellectual property rights.
  + Duration/Effort estimate: Monthly check taking about 2 hours per month.
  + Responsible party: Legal team
* **Loss of Data:**
  + Task: Implement regular data backups and disaster recovery plans.
  + Duration/Effort estimate: Setting up and testing the backups and recovery plan can take about 10 hours.
  + Responsible party: IT team
* **Legal Issues:**
  + Task: Ensure all website content adheres to copyright and intellectual property laws.
  + Duration/Effort estimate: Regular check taking about 2 hours per month.
  + Responsible party: Legal team
* **Technical Failure:**
  + Task: Conduct regular checks on the website's technical infrastructure to identify and address any technical issues proactively.
  + Duration/Effort estimate: Monthly check taking about 5 hours per month.
  + Responsible party: IT team
* **Server Downtime:**
  + Task: Ensure a reliable hosting provider with a robust service level agreement (SLA).
  + Duration/Effort estimate: Researching and selecting a reliable hosting provider can take about 20 hours.
  + Responsible party: IT team