|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **Threat** | **Existing Controls** | **Likelihood** | **Consequence** | **Level of Risk** | **Risk Priority** | **Suggested control** |
| Data Center | Power failure or environmental hazards | Backup power systems, disaster recovery | Rare | High | Medium | 1 | Regular testing of backup power systems |
| **Student Records** | Data hacked | Access controls, data encryption | Possible | Catastrophic | High | 2 | Implement multi-factor authentication for access to student records |
| Research Laboratories | Equipment malfunction or damage | Equipment maintenance, safety protocols | Unlikely | Moderate | Low | 3 | Regular equipment maintenance |
| **Academic Research** | Intellectual property theft or loss | Data access controls, confidentiality | Possible | Major | High | 4 | Implement strict access controls and data encryption |
| Cybersecurity Systems | Cyberattacks or data breaches | Firewalls, intrusion detection systems | Possible | High | Medium | 5 | Regular updates of security systems |
| **Student Health Services** | Privacy breaches or mishandling of data | Confidentiality protocols, access controls | Unlikely | Moderate | Low | 6 | Train staff on proper handling and protection of student health data |
| Network Infrastructure | Network outages or disruptions | Redundant network architecture | Unlikely | High | Medium | 7 | Redundant network connections |
| **Library Resources** | Theft or damage to books and materials | Security cameras, check-out procedures | Rare | Minor | Low | 8 | Implement a library security system and track check-out records |
| **Food Services** | Foodborne illnesses or contamination | Food safety protocols, inspections | Unlikely | Moderate | Low | 9 | Enforce strict food safety standards and regular inspections |
| Wireless Networks | Unauthorized access or network intrusion | Encryption, network monitoring | Possible | Moderate | Medium | 10 | Strong encryption and network monitoring |
| **Parking Facilities** | Vehicle theft or vandalism | Security patrols, surveillance cameras | Possible | Minor | Low | 11 | Increase security patrols and improve lighting in parking areas |
| Cloud Infrastructure | Data loss or security breaches | Data encryption, access controls | Unlikely | High | Medium | 12 | Regular data backups and access controls |
| **Student Activities** | Event accidents or injuries | Safety protocols, emergency response plans | Unlikely | Moderate | Low | 13 | Develop comprehensive safety plans for student activities |
| Computer Device Management Systems | Unauthorized access or data loss | Access controls, remote wipe capabilities | Possible | Moderate | Medium | 14 | Remote wipe capabilities for lost devices |
| **Environment** | Pollution or waste mismanagement | Recycling programs, environmental policies | Unlikely | Minor | Low | 15 | Promote and enforce sustainable practices across the campus |
| Technology Equipment Storage | Equipment damage or theft | Access controls, security measures | Unlikely | Moderate | Low | 16 | Enhanced physical security measures |
| **Emergency Response Plans** | The delay in the emergency response | Emergency drills, communication protocols | Unlikely | Major | Medium | 17 | Regular training and updating of emergency plans |
| Network Monitoring Systems | Network attacks or breaches | Intrusion detection, log analysis | Possible | High | Medium | 18 | Regular monitoring and log analysis |
| **Social Media Management** | Reputation damage or privacy breaches | Social media policies, monitoring | Unlikely | Moderate | Low | 19 | Social media usage guidelines |
| **Energy Management Systems** | Equipment failure or energy waste | Maintenance schedules, energy monitoring | Unlikely | Moderate | Low | 20 | Energy-efficient equipment and monitoring |
| Website | Website defacement or hacking | Web security measures, regular monitoring | Possible | Moderate | Medium | 21 | Regular website security audits |
| **Laboratory Equipment** | Malfunction or damage to equipment | Regular maintenance, equipment monitoring | Unlikely | Moderate | Low | 22 | Calibration and maintenance schedule |
| Email Systems | Email account compromise or phishing | Spam filters, email security training | Possible | High | Medium | 23 | Email security training and spam filters |
| **Student Privacy** | Unauthorized access or disclosure of data | Privacy policies, data protection measures | Unlikely | Catastrophic | High | 24 | Robust data encryption and access controls |
| Data Storage Systems | Data loss or corruption | Redundant storage, data integrity checks | Unlikely | High | Medium | 25 | Redundant storage and data integrity checks |
| **Campus Tours** | Accidents or incidents during tours | Safety guidelines, supervision | Unlikely | Minor | Low | 26 | Trained tour guides and safety protocols |
| **Student Financial Aid** | Fraud or mismanagement of financial aid | Financial aid controls, verification processes | Unlikely | Major | Medium | 27 | Strengthened verification processes |
| **Facility Maintenance** | Inadequate upkeep of buildings and grounds | Maintenance schedules, repair protocols | Unlikely | Moderate | Low | 28 | Implement proactive maintenance |
| **Study Abroad Programs** | Safety risks or emergencies abroad | Risk assessments, travel advisories | Unlikely | Major | Medium | 29 | Implement comprehensive safety plans |
| **Crisis Communication** | Ineffective communication during crises | Crisis communication plan, protocols | Unlikely | Major | Medium | 30 | Establish a dedicated crisis response team |