# **Asset Identification, Risk Assessment, and Risk Control Strategies**

# 

**Table 1: Inventory Worksheet**

|  |  |  |
| --- | --- | --- |
| **Assets** | **Data Classification** | **Impact to Functionality** |
| Student Interactivity | Private | **Medium** |
| VM Workstations | Private | **High** |
| Remote Connections | For Official Use | **Critical** |
| Services (Student VMs, Labs) | Confidential | **Critical** |
| Web Server (Outside Access to Blade) | Public | **High** |
| Application Server | Internal | **Critical** |
| Routing Devices | Public | **Critical** |

**Table 2: Weighted Factor Analysis Worksheet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assets** | **Criteria 1:**  **Impact to Revenue** | **Criteria 2:**  **Impact to Profitability** | **Criteria 3:**  **Impact to Public Image** | **Weighted Score** |
| *Criterion Weight (1-100)* | 30 | 35 | 35 |  |
| Customer Orders/Transactions | .90 | 1.0 | .95 | **95** |
| Customer Support via e-mail | .10 | .10 | .30 | **17** |
| Database Servers (Inventory Records, Distributor/Supplier Information) | .90 | .80 | .60 | **77** |
| Web Server (Organization’s Web Presence) | .40 | .70 | .80 | **63** |

**Table 3: Vulnerability Assessment**

|  |  |
| --- | --- |
| **Threat** | **Possible Vulnerabilities** |
| Software Attacks | Countless loopholes in software could open up a path for attack. A back door could be set up, providing easy access to customer and business information |
| Human Error | Employees or third-party workers could expose or throw away sensitive information without thinking. Will happen even with training. |
| Hardware Failure | Without proper backup, all records of transactions, shipping, and third-party partnerships with distributors/suppliers would be gone. The business would be crippled for an extended period of time. |
| Theft | Expensive in-store markers are highly popular. Someone who can’t afford one may go down to theft to obtain sought after item. Recovery will take time and look bad in public eye. |

**Table 4: Ranked Vulnerability Risk Worksheet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Asset Impact** | **Vulnerability** | **Vulnerability Likelihood** | **Risk-Rating Factor** |
| Database Servers (Student Project Designs) | 77 | Downtime of Inventory onto website due to hardware failure | .15 | 11.5 |
| Database Servers (VM Databases) | 77 | Back door through software attacks | .10 | 7.7 |
| Web Server (Organization’s Web Presence) | 63 | Maintenance out of site maintenance hours due to human error | .10 | 6.3 |
| Web Server (Organization’s Web Presence) | 63 | Server goes down due to DDoS | .15 | 9.45 |

**Table 5: Risk Control Strategies for Vulnerabilities**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Risk Control Strategy** | **Explanation** |
| Software Attacks | Defend | In order to fight off the loopholes within software, constant research must be done by the Info. Sec. team to keep up to date. Also, they are responsible for maintaining software updates that plug up these problems. |
| Human Error | Terminate | In order to remove as much human error as possible, training every six months will be **required** about security within an organization. On top of that, constant policy announcements and reminders will be throughout the organization to remind staff about security. Also, staff will be authorized based on level of access throughout **BOTH** facilities. These permissions will be assigned by the owners and security professional collaboration. |
| Hardware Failure | Mitigate | In case of a hardware failure, plans on recovering the data should be top priority. Methods such as backup and the exact problem of the failure shall be implemented as soon as possible. |
| Theft | Mitigate | Accurate planning must be priority with theft. If a theft does occur, we have to go through our inventory to see what is missing and calculate the cost. Also, the repair of any damage done to the organization must be attended to as soon as possible. If there is a presence of damage for an extended period of time, the public’s image towards the organization will slowly become negative. |

# **Enterprise Information Security Policy**

**Table 1: Enterprise Information Security Policy (EISP)**

|  |  |
| --- | --- |
| **Component** | **Description** |
| Statement of Purpose | In regards to the blade, our focus on security is number one priority whether it’s online or on site. Serious planning in recognizing our key assets and how to protect them are critical in the survival of this resource. Our main objective is to make sure that any risk that is apparent towards the blade is stopped immediately to ensure that our students will continue to have faith, trust, and respect towards the integrity of the blade. This mindset is constantly seen throughout the school with our elaborate, yet easy to understand policies. These policies make sure that every student, staff member, or faculty within the company realizes the seriousness of security, without making the work environment feel restricted. In short, security measures are not only to protect the blade from going down, but to prevent our students from doubting the capabilities of this great resource. |
| Information Security Procedures | Our school has multiple methods in regards to security. First, to prevent as much human error as possible, the organization’s policies are posted in multiple locations to give a friendly reminder of how important security is to the life of the blade. Also, training and education is performed every six months to ensure that individuals handling the blade are up-to-date with current trends regarding its safety.    Other methods include security cameras throughout the space to ensure security. These locations have key locks to prevent wandering individuals from accessing the blade. To ensure that individuals handling the blade don’t cause damage, we switch out roles of inventory check every month to catch potential “misplaced” items.    As far as protecting our digital information, elaborate firewalls, ACLs, and IDS and IPS have been implemented. This gives us the most confidence to tell students, and our partners that their information is kept as safe as possible. We also perform routine backups of our information off-site in case a natural disaster decides to occur. |
| Need for Security Procedures | Without the described procedures, the blade will fail. The blade is an upcoming resource that will aid students in learning material at a whole new level. This also allows faculty/staff to showcase this achievement to future students to spark interest both internally and externally. |
| Security Roles | To ensure that our security is at the highest standards, separate teams each with different skill sets have been assigned. First, our IT department is in charge of maintaining and securing all of our digital information that is essential to blade functionality. The experience staff working on the floor is in charge of maintaining general maintenance. They are equipped with keys which grant them access to the blade room. |

# 

# 

# **Business Continuity Strategies**

|  |  |
| --- | --- |
| **Successful Attack** | **Continuing Business** |
| Software Attack | If a software attack were to occur, our main goal would be to discover the point of entry. When we find the hole, we will either download the latest patches. If this were to have had happened before with the same software, then we would contact the company about the problem, and switch records to a new, more reliable software.  The best way to avoid as much hassle as possible, the first thing that should be done is to notify students affected about the minor delay via email or web page. Also, contacting all other individuals involved will keep them informed on the current situation. Once the problem is resolved and see what data was compromised, we notify whoever’s data was taken and help them as much as possible. |
| Human Error | Once a scene of human error is discovered, the first step is to go directly to the employee and ask what occurred. Once they tell you their mistake, quickly follow the trail to hopefully discover the error that occurred.  In the meantime, depending on the employee’s history, we will either retrain the entire staff about the error that occurred, or take disciplinary action. |
| Hardware Failure | If a hardware failure were to occur, our main goal would be to find the failed component. When we find the device, we will quickly replace it and if it were a server, copy over the data from the offsite backup. If this were to have had happened before with the same hardware, then we would contact the company about the problem, and switch records to a new, more reliable hardware.  The best way to avoid as much hassle as possible, the first thing that should be done is to notify students affected about the minor delay via email or web page. Also, contacting all other individuals involved will keep them informed on the current situation. Once the problem is resolved and see what data was compromised, we notify whoever’s data was destroyed and help them as much as possible. |
| Theft | If a theft were to occur, we would first look through all of the security camera footage around the estimated time of theft. We would then contact our security provider on when entry took place and if there was any action.  To compensate for stolen goods, we would have to use inventory to provide uptime. We would also have to repair the doors to maintain security. |