|  |  |  |
| --- | --- | --- |
| Section 1: | Alfred Private High School Information Security Policy | Effective Date: April 13, 2013 |
| Subsection | Organizational Security | Change Control #: 1 |
| Policy | Information Security Roles and Responsibilities | Approved By: Norman Greenbaum, Superintendent at Alfred Private High School |
| Objective | To establish the expected behavior of employees when dealing in with information security. |  |
| Purpose | The purpose of this policy is to ensure the security of all the information assets handled by this organization by communicating the functions employees of this organization plays in protecting data. |  |
| Audience | This policy applies to all employees, information owners and security professionals at Alfred Private High School |  |
| Policy | Each member of the organization will have a certain role in ensuring the security of information assets in this organization. It is critical that each member contribute to the security of the information assets. Therefore, it is to be expected that every employee abide by these behaviors. It is important for all roles to be included here because all members of the organization must understand the information security process in order to understand the part they play in it.    Employees: All teachers, culinary staff, administration staff, librarians, outsourced or third party contractors, and nurses will fill the role of employees.  Employees will be responsible for alerting information security professionals of any security risks they discover. Breaches of information security should be reported immediately. No action must be taken by the employee to mitigate the risk on his or her own. Immediately emailing, calling, or otherwise communicating to the information security professionals with a clear description of the observed risk is required.  Employees are responsible for attending information security training classes and events held by the information security professionals.    Information Security Professionals: All members of the IT department (at the time of writing of this policy, there are 5 IT employees) will fill the role of information security professionals.  Information security professionals are responsible for receiving and responding to reports of security risks delivered by employees. Receiving reports involves checking emails and voicemails at least once per day for new reports, and thanking the employee for his or her report. Responding to the report requires information security professionals to develop and execute a plan to mitigate the risk within five business days.  Information security professionals are responsible for holding at least one information security training class or event for employees per year. This event must involve all employees in the organization, and it must help employees look for security risks to report.  Information security professionals are responsible for designing information systems and developing information security policies for use by the organization that ensures appropriate confidentiality, integrity, and availability of information assets.    Information owner: This role will be filled by the superintendent.  The information owner is responsible for approving and enforcing information security policies. To approve a policy, the information owner must agree with all aspects presented by the policy after weighing the impact the policies will have on the organization’s functions and budget.  The information owner is responsible for designating a budget for securing information assets. |  |
| Exceptions | None |  |
| Disciplinary Actions | If any member of the organization is found to have willingly violated the contents of this policy, he or she will receive a written warning for the first offense. Upon the second offense by the same member, that employee will be terminated immediately.  If any member of the organization is found to have inadvertently violated the contents of this policy, he or she will receive a verbal warning for the first offense. The second offense, whether intentional or inadvertent, will result in a written warning. The third violation, whether intentional or inadvertent, will result in termination. |  |

|  |  |  |
| --- | --- | --- |
| Section 2: | Alfred Private High School Information Security Policy | Effective Date: April 13, 2013 |
| Subsection | Asset Classification and Control | Change Control #: 1 |
| Policy | Information Classification Policy | Approved By: Norman Greenbaum, Superintendent at Alfred Private High School |
| Objective | The objective of this policy will be to provide a way for Alfred Private High School to organize information assets by the potential risk those assets pose to the organization. |  |
| Purpose | Alfred Private High School will use an information classification system to determine the most effective use of resources for securing information. |  |
| Audience | The audience of this policy is all employees including teachers, nurses, custodial staff, culinary staff, administration staff, librarians, outsourced or third party contractors, and IT staff. All members of the organization that handle and interact with the information resources used by Alfred Private High School. |  |
| Policy | Alfred Private High School will implement a method to organize its information assets by the risk each asset poses to the organization. The method chosen must provide an effective way to communicate the importance of each information asset, as well as how to handle and label each asset, to all those who use the asset.    Each identified information asset in Alfred Private High School will be classified in one of four categories: public, restricted, sensitive, and confidential. The categories and their criteria may be changed by information security professionals within the organization after approval from the information owner.    All members of the organization must have knowledge of the meaning and criteria of each of the classifications. All information assets in the organization must have a clear label designating the classification. Each classification must have clear instructions for handling of assets. The instructions for handling must be communicated to all employees. |  |
| Exceptions | None |  |
| Disciplinary Actions | If any member of the organization is found to have willingly violated the contents of this policy, he or she will receive a written warning for the first offense. Upon the second offense by the same member, that employee will be terminated immediately.  If any member of the organization is found to have inadvertently violated the contents of this policy, he or she will receive a verbal warning for the first offense. The second offense, whether intentional or inadvertent, will result in a written warning. The third violation, whether intentional or inadvertent, will result in termination. |  |