Security Policy

John Jay
BEAUTY COLLEGE

2844 Tennessee Avenue,
Kenner, LA 70062

(504) 467-2774

Table of Contents

Introduction

The objectives of this security policy are to preserve the integrity of the data that has been entrusted to John Jay Beauty College and it's employees.

Users

This portion will introduce and break down the users in the network and their roles in securing data.

Jill Waguespack - Administrator
- FAFSA Security
- Student Information Security
- Student Grade Security

Shelly Laiche - Administrator
- Bookkeeping Security
- Payroll Security
- Employee Information Security

John Daigle - IT Security
- Makes changes to programs or systems

Acceptable Use

To ensure data confidentiality, all school owned computers will be used solely for educational and work related reasons. No mandatory changes shall be made to any school owned computer other than maintenance or updates performed by IT Security.

No personal use of computers will be tolerated in order to preserve the integrity of the data held on the school network.

This policy applies to but is not limited to:

- Office Administrators
- Employees
- Students

Authentication

To prevent unauthorized users from accessing information, all passwords will be specific to each employee and/or their respective department.

Administrators and employees are required to reset their password monthly.

Backup Policy

Backups are performed in the following intervals:

2 x Daily for workstations with 28 day retention - stored in the cloud
6 x Daily for server with 1 year retention - stored locally and replicated to the cloud

Confidential Data

Confidential data, including but not limited to:

- Bookkeeping
- FAFSA
- Payroll
- Student Grade Information
- Student Information
- Employee Information

should only be accessed by authorized administrators from school owned computers.

Network Access

Only school owned computers will have access to the private network “JohnJaySchool” , all other computers must use “JohnJayStudents” or “JohnJayGuest”, to prevent data being compromised on the network.

Network Security

Network security exists via firewall (Cisco), DNS Security (Cisco Umbrella), EDR (Sentinel 1), Windows Patch Management (RMM - N-able).

Security is solely administered and made changes to by:

John Daigle
Synergy Solutions, LLC - 3200 Ridgelake Dr., Suite 203 Metairie, LA 70002

Student Files
The administrators are responsible for all student files. Files are locked away and are only retrieved by administrators when necessary.

Files that no longer meet the legal requirement of 5 years to keep on file will be shredded and disposed of by administrators.

Any copies made of confidential information are filed or shredded and destroyed.

Training

Upon enrollment/hiring students and employees sign a contract agreeing to use all computers on the network properly. Students are provided education on “proper use” protocols and employees are given training on data security.

Security Breach Action Plan

In event of a security breach, IT Security will firstly be notified.

IT Security will immediately notify the administrators and work to secure the breach.

Security Review

Conducted by: Jill Waguespack _____Date: 5/5/2021

Area	Program Name	Last Reviewed	Reviewed By	Notes
Annual System Training	Employee training	5/5/2021	JW	Employees have been trained on how to properly secure confidential information
System Education	Student Education	5/5/2021	JW	All students have signed and agreed to proper use of all computers on the "JohnJayStudent" network, access to the "JohnJaySchool" network is restricted to any computers other than school owned computers
Strong Password	Employee management/information systems	5/5/2021	JW	Employees are required to change their user specific password every 30 days
System Access	Employee Management/Information Systems	5/5/2021	JW	All employee access has been reviewed, security around employee access has been verified.
Student Files	Storage	5/5/2021	JW	Administrators have verified files are secure and will remain locked until necessary
Back-up	Information Systems	5/5/2021	JW	2 x Daily for workstations with 28 day retention - stored in the cloud 6 x Daily for server with 1 year retention - stored locally and replicated to the cloud

Record Keeping	Records kept for the number of years required by law	5/5/2021	JW	Semi-annual review of all records is performed by administrators
Anti-Virus	All computers will have antivirus installed	5/5/2021	JW	Computers are equipped with antivirus software
Protecting Information	All confidential information will be sent through the auditor's portal	5/5/2021	JW	Administrators have been trained on the proper procedure for sending documents to auditors.

Risk Assessments:

Area	Risk Assessment	Date Reviewed	Reviewed By	Notes
All areas	Satisfactory	5/5/2021	JW	Executed by John Daigle, we will continue to review computers for any risks to security
Storage	Satisfactory	5/5/2021	JW	Training on record keeping will be executed semi-annually, 5 years of documents must legally be required and documents that no longer fit the criteria must be disposed of properly.