HEALTHCARE
CAREER COLLEGE

DATA SECURITY AND SAFETY PLAN 2019

REVISED: 3/20/2019

Table of Contents

INTRODUCTION

This *Data Security and Safety Plan* outlines the policies and procedures to be followed so that the school's technical infrastructure may be utilized in a safe and security way that protects the integrity of student data. Additionally, this plan outlines information for the technical infrastructure and resources used by Healthcare Career College.

DESCRIPTION OF ON-CAMPUS IT NETWORK INFRASTRUCTURE AND RELEVANT SECURITY PROTOCOLS

IT Network Infrastructure

Two server rooms are located on campus in suites #171 and #129. The server room is secure and temperature controlled for the protection of server hardware and to ensure network reliability. Only the IT Administrator and the Business Officer have access to the server room. The hardware is adequately maintained and upgraded to ensure network reliability. The IT/Network Administrator follows a procedure for backup of the school's database which is maintained on the server. Information stored on the Diamond SIS database is backed up by Diamond SIS.

Each employee is issued a unique user ID and login which they may use to access the network drives and computer systems.

The campus has three computer labs on campus in Suites #171, #203, and #129. Students do not have access to network drives or student information systems. Additionally, software cannot be downloaded on student computers.

Data Backup System

Backup for data stored on the school network is conducted daily from Monday-Saturday at 7:00pm. The daily backup data is stored in a hard drive Daily and monthly backup of the database conducted, so a snapshot of the system can be restored from last month. IT/Network Administrator checks the backup weekly to ensure that backups have been completed successfully. Any errors, if found, are resolved.

The monthly backup for the system is kept in a hard drive in a fire-proof, locked cabinet to secure the data. Additional backup for the entire network is completed on Friday evenings. entire network, including email and server data, is backed up every 24 hours. All data in Diamond SIS is backed up in real-time and stored on the Diamond SIS servers. Therefore, should power be lost locally, all data is saved and recoverable. Any issues regarding computer performance are reported immediately to the IT Network Administrator and handled within 24 hours.

SECURITY PROTOCOLS FOR ONLINE RESOURCES AND PROGRAMS

Faculty and staff may make use of online programs for school-related purposes. These programs include: DiamondSIS, Canvas LMS, Medcom, and EVOLVE. Each of these online programs has a data security policy which is kept on file. Any data transmission must only occur over these authorized systems so that data security may be maintained. Additionally, to mitigate any risk of data breach, each user only has access to the data relevant to their department.

USER INSTRUCTIONS AND PROCEDURES TO ENSURE THE PRIVACY, SECURITY AND SAFETY OF DATA

Healthcare Career College employees are issued a *Computer Use Policy* as part of their Employee Handbook. Student computer use policies are outlined in the School Catalog and posted in the computer labs. Ongoing employee training regarding secure use of the computer systems is provided by the IT/Network Administrator. Employee use of the computer systems is monitored daily by the IT/Network Administrators, and any potential security threats are addressed immediately.

DETECTION, PREVENTION AND RESPONSE TO ATTACKS, INTRUSIONS, OR OTHER SYSTEM FAILURES

Only school-authorized computer systems may be used by faculty and staff. All computer systems are equipped with an anti-virus software which monitors the systems continually for system threats. Daily reports from the anti-virus software are generated, which are monitored daily by the IT/Network Administrator. Any system failures are addressed within 24 hours, and backup systems are in place should the system restoration take longer than 24 hours.