Bellus Academy Campuses

Poway, CA
13266 Poway Rd|Poway, CA 92064 | 858-748-1490

OPE ID: 023434

Manhattan, KS
1130 Westloop Pl|Manhattan, KS 66502 | 785-539-1837

OPE ID: 02343401

El Cajon, CA
1073 E. Main St|El Cajon, CA 92021 | 619-442-3407

OPE ID: 012026

Chula Vista, CA
970 Broadway|Chula Vista, CA 91911 | 619-474-6607

OPE ID: 007050

Contents

DATA SECURITY PLAN (DSP)

This Data Security Plan for Bellus Academy describes safeguards to protect the confidentiality, integrity, and availability or our data, information, and technology assets. These safeguards are provided to:

- Enable due diligence to ensure the security and confidentiality of covered data, information, and resources
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of covered data, information, and resources that could result in substantial harm or inconvenience

This Data Security Plan also provides for mechanisms to identify and assess the risks that may threaten covered data, information, and resources. Manage and control these risks; implement and review the plan; and adjust the plan to reflect changes in technology, the sensitivity of covered data, information and resources, and internal or external threats to information security.

ACADEMY / ORGANIZATION REQUIREMENTS (BUSINESS, FUNCTIONAL AND TECHNICAL)

ELEMENT	DESCRIPTION
Employee Management and Training (Data Security Coordinator)	The Data Security Coordinator is responsible for new and existing employee training on the cyber security policy and protection of company/student data covering the following required topics. The Data Security Coordinator meets monthly with the internal IT team and the external IT support company FIT Solutions. The FIT Solutions company provides training and information to the Data Security Coordinator on areas of data and information protection. **Responsibility for Company Data** Bellus Academy employees are trained on the critical nature of data security and the responsibility of each employee to protect company/student data. **Document Management and Notification Procedures** Bellus Academy employees are educated on data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). Employees are trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident to the IT Director to engage and mitigate and investigate the threat.

Passwords
Bellus Academy employees are trained on the minimum password requirements and the frequency of password changes while using company data systems.

Unauthorized Software
Bellus Academy Employees are informed they are not allowed to install unlicensed software on any company computer. Unauthorized software downloads could make our company susceptible to malicious software downloads that can attack and corrupt company data. The ability for end users to install any software on company computers is provided only according to least privilege; when required for their business duties. Persistent monitoring is performed to detect the installation of malicious applications or those not germane to business functions.

Internet Use
Bellus Academy employees are trained to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data.

Email
Bellus Academy employees are trained on email usage and the threat posed by unauthorized emails (emails received that they do not recognize). This includes ensuring that emails

- Comes from someone they know
- Comes from someone they have received email from before
- Is something they were expecting
- Does not look odd with unusual spellings or characters
- Passes our anti-virus program test

Social Engineering and Phishing
Bellus Academy employees are made aware to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

Mobile Devices
Bellus Academy Employees are trained to understand the mobile device company use policies including the understanding that mobile devices are only authorized on the company network for use in the normal work requirements of their job duties. Even when leveraging mobile devices, access to Bellus informational resources is constantly monitored for intrusions and anomalous behavior.

Protecting Computer and Network Resources
Bellus Academy employees are trained on safeguarding of their work computers and devices from theft by keeping them locked and in a secure place.

Physical Security	Bellus Academy has addressed physical security by placing access restrictions to the building, computers, and records storage facilities, information, and resources to permit access only to authorized individuals.

	Only authorized employees are permitted to possess keys or combinations. Paper documents containing covered data and information are to be shredded at time of disposal.
Information Systems	Access to covered data, information, and resources is limited to those employees who have been trained and have a business reason to know such information. Each employee is assigned a set of unique credentials. Databases containing personal covered data, information, and resources including, but not limited to, accounts, balances, and transactional information are available only to employees in appropriate departments and positions. BELLUS ACADEMY will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data, information, and resources are secure and to safeguard the integrity of records in storage and transmission. Authentication is also required of users before they can access system-protected data. In addition, security systems have been implemented to assist with detection and mitigation of threats, along with procedures to handle security incidents if they should occur. Encryption technology will be utilized for both storage and transmission. All covered data, information, and resources will be maintained on systems that are behind a firewall. **Firewalls** Chula Vista: Meraki MX64 El Cajon: Meraki MX64 Manhattan: Meraki MX84 Poway: Meraki MX84

Management of System Failures and Compromises	1. Bellus Academy has developed plans and procedures to detect actual or attempted attacks on the academy's systems and has an Incidence Response Plan in place which outlines procedures for responding to an actual or attempted unauthorized access to covered data, information, or resources. Incidence Response and Reporting procedures are detailed later in this document.
Anti - Virus	1. All Bellus Academy systems must have anti-virus software installed. All systems have virus protection installed on all computers connected to the campus computer network. 2. The anti-virus software and the virus definitions must be kept up- to-date. Anti-virus software is updated and maintained by FIT Solutions our IT support company. 3. Virus-infected computers may be removed from the network until they are verified as virus-free. 4. The System Administrator is responsible for creating procedures that ensure anti-virus software is in place, operating correctly, and computers are virus-free. This is all managed through our IT company FIT Solutions. 5. Any activities with the intention to create and/or distribute malicious programs into BELLUS ACADEMY networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited. **Antivirus** Sophos Central Endpoint. All virus definition updates are all handled in the cloud for each endpoint and are automatically updated by Sophos.
Network Control and Access	1. Anyone who uses the computers must be properly authorized. 2. Users must not: • Perform acts that negatively impact the operation of computers, peripherals, or networks or that impedes the ability of someone else to do his/her work. • Attempt to circumvent protection schemes for access to data or systems. • Gain or grant unauthorized access to computers, devices, software, or data. 3. Users may be held legally and financially responsible for actions resulting from unauthorized use of BELLUS ACADEMY's network and system accounts. 4. BELLUS ACADEMY has installed various network security devices, including account passwords and firewalls, to help ensure the safety and security of information. Any attempt to disable, defeat or circumvent any security facility is considered inappropriate activity and is a violation of this network policy.

	5. Expansion or manipulation of network hardware and/or software, except by designated individuals by management, without prior approval from management, is strictly prohibited. 6. Static assignment of IP addresses not approved or obtained through management is prohibited. 7. Only members of management or authorized agents may move BELLUS ACADEMY-owned networking and communications equipment. 8. The owners of data stored on network accessible systems are responsible for managing and determining the appropriateness of information stored on these systems. This includes both private storage areas and "shared" folder areas.
Security Assessment	1. Network and system security will be assessed on a periodic basis. 2. Security testing and audits will be conducted by our IT company, Fit Solutions on a quarterly basis. 3. If a security concern is found, the responsible party will be notified so the problem can be addressed. Depending on the severity of the concern the device may be removed from the network.
End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)	1. Users are responsible for the security and integrity of BELLUS ACADEMY's information stored on their end-user devices, which includes controlling physical and network access to the equipment. This includes personally owned devices to the extent they access BELLUS ACADEMY's IT services or contain the academy's data of any kind. Storage of confidential or personal covered data on mobile devices is strictly prohibited. 2. Users may not run or otherwise configure software or hardware which may allow access by unauthorized users. 3. Employees must not access BELLUS ACADEMY-owned end-user devices which have not been provided to them for their work without the express permission of management. 4. Employees accessing BELLUS ACADEMY's IT services and systems with their own personal devices must adhere to all IT polices. 5. Fit Solutions installs anti-virus software on all workstations/laptops that connect to BELLUS ACADEMY's network.
Software Licenses	1. Virtually all commercially developed software is copyrighted; and the users may use it only according to the terms of the license that BELLUS ACADEMY obtains. 2. Duplicating such software with the intent to redistribute or installing multiple instances of such software without authorization is prohibited. 3. All users are legally liable to the license issuer or copyright holder.

4. Placing unlicensed or illegally obtained software, music, movies, or documents on BELLUS ACADEMY's computers is strictly prohibited.

Physical Access

1. Electronic data is protected via the data center. During transmission and storage electronic data is encrypted. During storage traditional data (paper surveys) are stored within a locked file container within a locked office.

2. Access should only be granted to any person with proper authorization to access the corresponding area.

3. Unauthorized access to areas where personally identifiable information is stored is prohibited and prevented by locks.

4. Management must ensure that staff who (voluntarily) terminate their employment with the department return their physical access keys and codes on their last day of work.

5. Employees who are (involuntarily) dismissed from BELLUS ACADEMY must return their keys and other access control devices/codes at the time they are notified of their dismissal. Any access granted to access control devices/cards are removed immediately.

6. If an employee does not return his/her keys, areas controlled by the outstanding locks are re-keyed for information protection.

7. BELLUS ACADEMY information or records may not be removed (or copied) from the office where it is kept except in performance of job responsibilities.

8. Access to BELLUS ACADEMY's IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance.

9. Adequate disaster recovery plans and procedures are required for critical systems data.

Systems	1. Administrative access to servers containing or processing protected data must be password protected. 2. Servers are physically located in an access-controlled environment. 3. All servers deployed at BELLUS ACADEMY must be approved by management. System maintenance plans must be established and maintained and approved by management. 4. Network Services are kept up-to-date with any changes to system information. 5. Operating system configuration should be in accordance with approved security best practices. 6. Services and applications which will not be used must be disabled where possible. 7. Access to services are logged using a ticket system and/or protected through access-control methods if possible. 8. The most recent patches must be installed on the system as soon as practical. 9. Do not use accounts with elevated privileges (such as administrator) when a non-privileged account can be used. Do not use unsecured/unencrypted protocols (such as telnet or http) when secured protocols (such as SSH or HTTPS) can be used. 10. Audits may be performed on any device utilizing BELLUS ACADEMY's Network resources at the discretion of management. 11. Privileged access must be performed via an encrypted network.
Passwords	1 Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords. 2 Passwords changes are required immediately if compromised. Passwords should be memorized and never written down. 3 Passwords should not be stored in electronic form – in computer files or on portable devices such as USB memory keys unless strongly encrypted. 4 Password "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users will be locked out of systems after 5 unsuccessful attempts. 5 Computer log-in password are required to be updated annually.

	6 Computer log in passwords are required to consist of at least 7 characters, including at least 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.
System Backup	Full backups along with a snapshot are performed at a minimum daily. 1 Bellus is utilizing Datto for backups. Datto creates a snapshot of each server every 60 minutes. All backups are also replicated to the Datto cloud in the event of an onsite failure. Backups in the cloud can be spun-up and accessed remotely.
Physical Assets	1. Networking and computing hardware should be placed in a secure environment and space shall be dedicated to their functions whenever possible. 2. Employees must know where the fire suppression equipment is located and how to use it. 3. Materials should not be stored on top of or directly next to equipment; proper airflow and environmental conditions must be maintained.
Wireless Access	1. This policy strictly prohibits access to network resources via open, unsecured wireless communication mechanisms. 2. Wireless access points not sanctioned by BELLUS ACADEMY are prohibited.
Destruction and Disposal of Information and Devices	1. Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded. 2. When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that confidential data is rendered unreadable. Any confidential information stored must be thoroughly destroyed. In general, it is insufficient to "delete" the information, as it may remain on the medium. The data should be properly removed from the drive either by software meeting U.S. Department of Defense specifications or by physically destroying the drive.
Security Monitoring	Fit Solutions performs internal and external security audit. The scans will report potential vulnerabilities. This will be done in real-time by an internal sensor. MSSP, FIT Cybersecurity, performs 24/7 monitoring of network activity, potential intrusion, operating system logs, application logs, and assets, and provides real-time incident response.

Incident Reporting

1. Any actual or suspected security incident involving unauthorized access to electronic systems owned or operated by BELLUS ACADEMY.
2. Malicious alteration or destruction of data, information, or communications.
3. Unauthorized interception or monitoring of communications.
4. Any deliberate and unauthorized destruction or damage of IT resources.
5. Unauthorized disclosure or modification of electronic BELLUS ACADEMY or personal information. Incidents will be treated as confidential unless there is a need to release specific information.

Incident Response

BELLUS ACADEMY's IT/Technology Director is the primary point of contact for responding to and investigating incidents related to misuse or abuse of BELLUS ACADEMY's Information Technology Resources. This includes computer and network security breaches and unauthorized disclosure or modification of electronic BELLUS ACADEMY or personal information.

Upon discovery of a security breach, provide initial notification of the breach to:

Name: David Yocum

Title: IT/Technology Director

Phone Number: 785.410.5966

Management will then take steps to:

- Inform local law enforcement or the state attorney general as appropriate.
- Report stolen finances or identities and other cyber-crimes to the Internet Crime Complaint Center at www.ic3.gov
- Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov
- Report to the Department of Education within 24hrs of finding there has been a breach.
- Report to our accrediting agency, NACCAS within 24hrs of finding there has been a breach.

Steps to follow in case of an incident (Information law enforcement will need):

1. Create a log of all actions taken and maintain this log consistently throughout the incident response process.

2. Secure the affected area(s). Electronic evidence can be easily destroyed, resulting in the inability to determine if confidential information has been compromised or to provide evidence for future prosecution. Identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. For example, do not alter the condition of any electronic device by either turning it on, off, or rebooting it until it is determined that it is safe to do so. Inventory and evaluate the scene.
3. Assess the need for forensic information, such as that gathered from packet traces and system monitoring utilities, which can aid in understanding the nature and scope of the incident and provide evidence for any potential criminal investigation. During this process, consider both the potential value of forensic information vs. the immediate need to protect and restore BELLUS ACADEMY resources and services. Document the decision process.
4. Collect and save any forensic information identified in the previous two steps. This may include video records, access logs, system logs, network traces, IP addresses, MAC addresses, data backups, system images, or affected computer hardware.
5. Regain control of the compromised system. This may include network disconnection, process termination, system shutdown, or other action as indicated to prevent further compromise of protected information.
6. Analyze the intrusion. Document the nature of the intrusion and its impact on information and process integrity. Determine if unauthorized individuals may have acquired restricted information. Attempt to determine the identity of those whose data may have been acquired. Estimate the potential cost (in time, money, and resources) of the intrusion to BELLUS ACADEMY.
7. Correct any identifiable system or application vulnerabilities which allowed the intrusion to occur.
8. Verify system and data integrity.
9. Restore service once the integrity of the system and/or information has been verified.
10. The Director shall create an incident report with all relevant information. The report should include:
    - Date and time the incident occurred;
    - Description of incident;
    - Detailed list of system(s) and data which were compromised;
    - Identifiable risks to other systems or information;
    - Corrective actions taken to prevent future occurrences;
    - Estimated costs of incident and any corrective actions;

- Identity of those responsible for the incident (if available).

SENSITIVE DATA PROTECTION

Special care and awareness is required with regard to "sensitive data." Sensitive data is any which the unwarranted and/or unauthorized disclosure of such would have an adverse effect on BELLUS ACADEMY or individuals to which it pertains. Unauthorized disclosure or mishandling of sensitive data can be a violation of federal and state law and BELLUS ACADEMY and its employees can be held personally liable for damages or remediation costs.

Data related to identity theft such as social security number (SSN), credit card numbers, bank account information, driver's license, name, address, birthdate, passwords, Personal Identification Numbers (PINs), and ID pictures are of particular concern as all or most of this information is collected in the course of business. Other types of data such as medical information, tax returns, donor information, mailing lists, scholarship information, financial information, and bidding information are examples of data which could require confidential handling or restricted access. These examples are not exhaustive or all inclusive. It is the responsibility of the academy's employees handling any sensitive data to understand what data is sensitive and confidential and to adhere to the following guidelines and any applicable regulations:

- Data should be stored in as few places as possible and duplicated only when necessary.
- Inventory and identify the data under your control which is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner to minimize risk.
- Do not store confidential data on or copy it to mobile, external, and/or removable storage devices. This may include smartphones, tablets, or any other device that could easily be lost, stolen or compromised.
- Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data.
- Transmission and storage of any sensitive data should be encrypted.
- Release of BELLUS ACADEMY data to 3rd Parties - Do not release BELLUS ACADEMY data of any kind to 3rd party, non- BELLUS ACADEMY entities for any reason, unless such entities have agreed in writing to restrict the use of such data to the specific and intended purposes authorized by BELLUS ACADEMY management enlisting the services of the 3rd party entity. Any BELLUS ACADEMY employee releasing data to a non- BELLUS ACADEMY 3rd party entity is responsible for how the data is used (misused). Release of highly sensitive and confidential data (beyond FERPA allowed "directory information") is prohibited.
- Do not send, receive, or store any sensitive data using email under any circumstances. unless the emails and attachments are secured using end-to-end encryption and any documents password protected.
- Report any breaches, compromises, or unauthorized/unexplained access of confidential data immediately to the Director.
- All traditional data (paper surveys) must be kept in a locked file container within a locked room when not occupied or in use by an authorized person(s).

MFA

- Bellus is using Microsoft MFA to provide two-factor authentication for all Bellus email accounts. Users can use a text, phone call or the authenticator app to provide the secondary authentication. The Outlook application utilizes an app password to securely connect it to Office 365.

Email Filtering

- Bellus utilizes MXGuardDog to filter all emails into the accounts. This blocks SPAM and potentially harmful emails from being delivered to user's mailboxes. Users are then provided a quarantine report to release or remove any caught emails. Due to the potential for all technical email filtering controls to fail, email filtering is supplemented by robust security awareness training of end users.

PRIVACY STATEMENT

BELLUS ACADEMY endeavors to ensure that its treatment, custodial practices, and uses of "Personal Information" are in full compliance with all related federal and state statutes and regulation.

1. The academy commits to take reasonable precautions to maintain privacy and security of students' and employees' personal information. BELLUS ACADEMY cannot guarantee that these efforts will always be successful; therefore, users must assume the risk of a breach of BELLUS ACADEMY's privacy and security systems.
2. BELLUS ACADEMY does not intend to sell, or otherwise disclose for commercial purposes, outside the scope of ordinary BELLUS ACADEMY functions, students' and employees' name, mailing address, telephone number, e-mail address, or other information. While BELLUS ACADEMY makes reasonable efforts to protect information provided to us, BELLUS ACADEMY cannot guarantee that this information will remain secure and are not responsible for any loss or theft.
3. Personally, identifiable information is defined as data or other information which is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information known about them. All such data is stored in compliance with applicable laws.
4. Personal information includes, but is not limited to, information regarding a person's social security number, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, gender, race, religion, political affiliation, personal assets, medical conditions, medical records, and personnel or student records.
5. Some data items are considered directory information and will be released to the public unless a request is filed to prevent disclosure of the information, except for any other reason than official BELLUS ACADEMY business. Employees who request confidentiality of that information should contact management; and students should contact the Director.
6. BELLUS ACADEMY assumes that failure on the part of any student or employee to specifically request the withholding of categories of information indicates individual approval for disclosure.
7. BELLUS ACADEMY is bound by the Family Educational Rights and Privacy Act (FERPA) regarding the release of student education records, and in the event of a conflict with BELLUS ACADEMY policies, FERPA will govern.