

# Information Security Overview

**Security Matters:**

Information is our most important asset and maintaining trust is vital to our students, faculty and staff. Not only is there an expectation to process the information we hold safely and securely, but laws and regulations dictate that San Joaquin Valley College, Inc. (SJVCi) employ policies, controls and education that support the data we handle. SJVCi includes San Joaquin Valley College, Carrington College, Santa Barbara Business College, and Ember Education. Security breaches have many negative impacts on individuals as well as the business and brand.

**How to get support:**

If you have any questions or concerns do not hesitate to contact out security team directly at security@embered.com or 800.530.7244 and we will be able to assist.

**Types of information we protect:**

 Personally Identifiable Information (PII): Information that can be used to identify, contact or locate an individual.

* Name (First and Last), Address, Phone Number, Email Address

 Sensitive Personal Information (SPI): Information that can be used for financial verification, financial transactions or is governed by privacy laws.

* Social Security Number, ID Number, Credit/Debit card number, demographics, health information and passwords

**Information Handling and Use:**

Information we collect, process and store must only be used for the intended purpose it was collected. Access to information is controlled so only the individuals that need access are provisioned access. Do not attempt to access systems or information that you have not been granted rights to use or view.

**Physical Security:**

The primary function of the physical security of our campus is to protect students, faculty and staff wellbeing. Physical security is also important to protect printed information and information stored within our systems. Hardcopy information that is PII or SPI must be stored in locked rooms or file cabinets. When disposing of printed information that contains PII or SPI you must use the secure disposal bins. Computers, printers and other associated technology must be secured in a manner that they are not accessible to the public or unauthorized individuals. Laptops, tablets and phones also need to be secured in the office and away from the office. If you must leave a device in your vehicle secure it in the trunk or otherwise out of sight.

**Account Security:**

Your account is what identifies you and any activities you take within a system. It is your responsibility to protect usernames, passwords and security questions. In the event you believe your credentials may be compromised please contact support immediately so we can assist.

**Passwords:**

Never share your passwords with another individual, never write down your passwords or store them in insecure locations. Create passwords that are complex and not easily guessed. It is highly encouraged that you use a password manager like KeePass or Lastpass as well as using a different password for each system, this includes personal passwords for social medial, e-commerce and personal email.

**Email Security:**

Email is one of the primary sources of data loss, computer viruses, and electronic attacks. SPI must not be sent in email; emails can easily be sent to unintended recipients and in the event an attacker gains access to a mailbox this information would be unprotected. We have put extensive controls in place to protect email, but attacks evolve at a much faster rate than the protections available. Do not open any messages from unknown sources, messages that look suspicious or messages with unexpected attachments. Attackers regularly attempt to spoof messages appearing to be from others within the organization but include malicious links or attachments. If you receive a suspicious message report it immediately.

**Viruses and malware:**

Security software is deployed to all workstations and servers. Any attempt to uninstall or disable security software is not permitted. Tampering with security software exposes not only the business but also your personal information to attack. If you suspect your computer has been infected with a virus or the security software has stopped functioning report it immediately.

**Social Engineering:**

Malicious individuals will go to great lengths to try to gain access to information by impersonating leadership, staff, or other individuals such as law enforcement and vendors. Do not communicate with anyone that seems suspicious, especially if they are attempting to engage in a financial transaction such a wire transfer, purchase of gift cards or crypto currency. Do not share personal details with unknown or suspicious individuals as these may be used are part of a larger attempt to gain access to your accounts. This includes usernames, passwords, PIN numbers, and security question answers. Report any suspicious phone calls, mail, or e-mail immediately.

Version 1.1

7/24/2020