IS and Physical Security Policy

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 the Organization protects

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

The electronic communication systems are not secure and may allow inadvertent disclosure, accidental transmission to third parties, etc. Sensitive information should not be sent via unsecured electronic means.

Account Security

An employee's account is what identifies them and any activities they take within the information system. It is each employee's responsibility to protect usernames, passwords and security questions. In the event an employee believes their credentials may been compromised, they are directed to email or number identified above immediately.

Passwords

Never share company passwords with another individual, never write down your passwords, or store them in insecure locations. Create passwords that are complex and not easily guessed, such using phrases. It is highly encouraged that employees use a password manager like KeePass well as using a different password for each platform.

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. The Organization's systems 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 an employee receives a suspicious message, they are required to report it immediately by forwarding the suspicious email to: email.security@embered.com.

Viruses and malware

Security software is deployed to all workstations and servers. Any attempt to uninstall or disable security software is prohibited and may result in corrective action up to and including immediate separation of employment. Tampering with security software exposes not only the business but also the user's personal information to attack. If an employee suspects their computer has been infected with a virus or the security software has stopped functioning, they are required to report it immediately to security@embered.com.

S*ocial 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 as 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 an employee's accounts. This includes usernames, passwords, PIN numbers, and security question answers. Report any suspicious phone calls, mail, or e-mail immediately to security@embered.com.

Physical Security

The primary function of the physical security of our campuses and offices is to protect the wellbeing of students and employees. Physical security is also important to protect printed information and information stored within the Organization's 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.

Policy Violations

Violations of this policy could expose the Organization to significant operational risks and may result in corrective action being taken against the employee.

The electronic communication systems are not secure and may allow inadvertent disclosure, accidental transmission to third parties, etc. Sensitive information should not be sent via unsecured electronic means.