**Password Policy**

**Purpose:**

To establish a standard for creation of strong passwords, the protection of those passwords, and the frequency for changing those passwords.

**Policy:**

1. Password construction
	1. All passwords must conform to this policy.
	2. Users must not use the same password across all accounts.
	3. Users must not use the same password for [Insert Covered Entity or Business Associate name] accounts as personal accounts.
	4. Each user’s password should meet the minimum requirements as outlined below (determine which requirements your organization will use):
		1. Must be a minimum of eight characters in length.
		2. Must contain a unique character.
		3. Must contain a number.
		4. May not contain your username or any part of your full name
		5. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
	5. Passphrases are better used than passwords.
2. Password change (determine which requirements your organization will use)
	1. All passwords will be changed every 90 days.
	2. If a password is compromised, the Security Officer will be notified and the password will be changed immediately.
	3. Users may not reuse the last five passwords.
3. Password protection
	1. Passwords must not be shared with anyone.
	2. Do not write down passwords and do not post them anywhere.
	3. Do not store passwords in documents that are not encrypted.
	4. Do not use the “remember password” feature on applications.
	5. Do not send passwords through email.
	6. Do not reveal passwords over the phone.

**Violations:** Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.