**Blue Team X**

**POLICY & PROCEDURES**

### **Password Management**

### **Effective Date:** <Month Day, Year> **Rev.** 1

**Policy:** We must develop, implement, and regularly review a formal documented process for appropriately creating, changing, and safeguarding passwords used to validate a user's identity and establish access to our information systems and data. All of our workforce members must be regularly trained and reminded about this process.

**Procedures:** We train and remind our workforce members about our process for creating, changing and safeguarding passwords used to validate a user's identity to access our information systems. Passwords will be changed from time to time and must not be shared with anyone else or ever displayed in open view. No workforce member may request another workforce member to reveal their password.

**Details:** The password management procedures include but are not limited to:

* Workforce members receive training on what to do if their password does not work.
* Require use of individual passwords to maintain accountability.
* Initial passwords are required to be given to users in a secure manner.
* Workforce members select and change their own passwords.
* Non-IT Employees
  + Passwords must have a minimum length of eight characters, if possible.
  + Password must be changed every 60 days.
  + Passwords cannot be reused during within a 180 day period.
* IT Staff
  + Passwords must be a minimum of 16 characters. (Passphrases are preferred but not required) Passwords can be randomly generated or user created.
  + Passwords must be changed every 30 days
    - in the event of a security breach, minimum change time will be every 60 minutes
* Passwords should not be based on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports team, etc.).
* Passwords must be composed of a mix of numeric and alphabetical characters.
* Passwords will not be displayed in clear text when being input into a software application.
* Default vendor passwords are required to be changed following installation of software.
* Password management training will cover topics such as:
* Keeping passwords confidential and not sharing them with others.
* How to avoid maintaining a paper record of passwords, unless the record can be stored securely.
* How to change passwords whenever there is any indication of possible information system or password compromise.
* Changing temporary passwords at the first logon.
* Reporting password concerns.
* Documentation (e.g. training materials, policies and procedures) of the practices in place will be retained as evidence of compliance.