**Account creation Policy**

Policy for creating and resetting new user accounts

1. **Purpose**
   1. The purpose of creating a user account is to ensure that the user in our online environment is validated and allowed access into our workstations. These workstations include: Laptops, Desktops, Cellphones, Servers, and Online applications.
2. **Scope**
   1. This information is used for every new account made with in the company. All other general policy’s that apply with the dealing of sensitive information should still apply for new account information.
3. **Account creations**
   1. Account creation will be done manually by someone in our I.T. department.
   2. The username of accounts should be first name underscore last name and last for digits of your employee ID number. Example Firstname\_Lastname#### or Cody\_Stitt6804. This not only makes each username unique but also eliminates the problem if two people have the same first name and last name.
   3. Every new account that is made will have a default password which will be changed the first time the user logs into the account.
   4. Accounts will have a security question tied to the account for verification if there ever need to be any maintenance is needed to be done on the account.
   5. Information that links the users to the account is their name, date of birth and employee ID. Their Employee ID is linked to their name, date of birth, address, and SSN.
4. **Password management** 
   1. Passwords should contain all of the following:
      1. No less than 6 characters but no more than 18.
      2. Must contain at least one Number.
      3. Must Contain at least one special character (e.g.,!@#$)
      4. Must contain at least one upper case character.
      5. New password cannot be the same as the last 3 passwords.
      6. Passwords will expire after 180 days.
      7. Notification to reset password before expiring will happen 30 days before password expiration data.
5. **Password reset and account lock out**
   1. If a user needs to reset their password they can do so without the assistance of a human. They would need to verify their name, employee ID number, and the current password. This is for when the user is changing their password before the expire date.
   2. If a user does not remember their password they can do also do so with out assistance of a human. They would need their name, date of birth, employee ID, and the security answer.
   3. After 5 failed attempts to login, the account will lock.
   4. Locked account will need to be manually unlocked. A user will have to call the IT to have accounts unlocked and password changed.