PPI Security Policy

We need to pay close attention to the handling of Protected Personal Information (PPI), not only to protect employee and customer private data, but also because this is a legal requirement under state and federal statutes.

What is PPI? PPI is defined as:

> First and last names with Social Security or other government ID number
>
> Or
>
> Financial account information including bank accounts, debit cards, and credit cards

PPI Access and Storage

PPI Physical Files

- **What's required?** PPI physical files must be stored in locked cabinets with access restricted to those with direct administrative responsibility. If confidential information is handled via physical mail, it must be delivered to and from a secure locked location.
- **Who does this apply to?** All employees
- **Who is responsible?** Jane Doe
- **What's the penalty if it's not done?** Written warning for employee file

PPI Electronic Files

- **What's required?** PPI electronic files must be stored in a secure server location with access restricted to users requiring access for the purpose of dissemination, distribution or processing.
- **Who does this apply to?** All employees
- **Who is responsible?** Jane Doe
- **What's the penalty if it's not done?** Written warning for employee file

PPI Distribution

- **What's required?** If protected or confidential information needs to be distributed outside of the domain boundaries, it must be distributed through a secure connection. A secure connection is defined as an encrypted connection and protected transfer site; or, if e-mail is required, mail must be encrypted outside of the secure domain environment. In all instances where feasible, please use fax or telephone to transmit protected data.
- **Who does this apply to?** All employees
- **Who is responsible?** Jane Doe
- **What's the penalty if it's not done?** Written warning for employee file for first offense and performance review impact for each violation thereafter

Account and Access Security Requirements

Passwords

- **What's required?** Users are prompted automatically to change passwords every 90 days. Passwords must be complex containing three character sets (upper case, lower case, numbers, and/or special characters). The last password cannot be reused for six password refreshes. After four incorrect attempts to login, the account is locked out for a period of not less than five minutes.
- **Who does this apply to?** All employees
- **Who is responsible:** IT Department
- **What's the penalty if it's not done?** Configured on applicable server. Written warning for employee file for first offense and performance review impact for each violation thereafter

New Logins and Accounts

- **What's required?** For new employees, or employees requiring a new login, an account is created with a unique user name and unique password. The password is required to be changed on first logon. For new employees requiring physical access to protected or confidential information, a key or card key is distributed and the employee will log and sign for the acceptance of the key or card key.
- **Who does this apply to?** All employees
- **Who is responsible:** IT Department
- **What's the penalty if it's not done?** Configured on applicable server. Written warning for employee file for first offense and performance review impact for each violation thereafter

Terminated and Retired Accounts

- **What's required?** In the case of termination or retirement of an account, the account is placed into a retired account Organizational Unit and all access rights are removed. The retired account Organizational Unit will actively deny access to domain resources. Any physical access capability such as keys or cardkeys will be retrieved immediately at the time of the terminated employment. If employee handles personal protected information, keys and/or keycards must be received within 24 hours of termination. If not received within 24 hours, all access codes belonging to the terminated employee will be disabled and physical locks changed.
- **Who does this apply to?** All employees
- **Who is responsible:** IT Department
- **What's the penalty if it's not done?** Configured on applicable server. Written warning for employee file for first offense and performance review impact for each violation thereafter