Bud Werner's Password Protection Program

Draft Policies

1. Mandatory that all staff machines use the service. No exceptions.
2. All browsers will be set to never remember login information outside of LastPass.
3. Staff will no longer allow websites to remember their login information.
4. Master Passwords will be generated using the Diceware method and will be updated annually.
5. Master passwords will be shared with supervisors if they deem it necessary. These will be maintained in a secure note.
    - Supervisors will check quarterly to ensure that they can access their staff's accounts if they have asked for master passwords
    - Supervisors may also ask that staff store their passwords in one main folder and share that folder with their supervisor.

1. Once all logins are input, weak passwords must be updated with auto-generated passwords offered by the software
2. When creating new logins staff must use the auto-generated passwords offered by the software. No making passwords up. No re-using of passwords.
3. With the exception of Sierra, service desks will never know the master passwords to their machines, and they will never be given passwords to the software they use unless they are given personal accounts.
4. Login information can no longer be written down on a piece of paper or maintained in a binder.
5. All in-house passwords are managed via BWML email accounts.
6. Personal passwords must be maintained on a separate LastPass or KeePass account.
7. No staff may save personal passwords to their BWML account
8. Login information will never be shared via email.

Administration Settings

- Admin can reset any master password and thereby login to that account and capture passwords
- Trusted account browsers are set to never remember master passwords
- Trusted account users are automatically logged out after 10 minutes of inactivity or after a browser has been closed or inactive.
- All accounts are prohibited from exporting data except the admin.
- Last Pass Support Center: https://lastpass.com/support.php

Individual Trusted Accounts – Department Heads & Support Staff

1. Each Use their staff BWML email account
    - master password is given to their supervisor if they are not a DH member and if the supervisor feels it is necessary.
2. Each staff machine will be set up with LastPass access
3. Each staff account will be given access to the logins necessary to that staff person and their department
4. When staff leave, their access is removed, but BWML keeps the login data.
5. All passwords in a trusted account should be changed by the supervisor upon the employee leaving.

Service Desk Accounts

1. Each Use a different generic BWML email account.
    - master password maintained by supervisor
2. Each staff machine would be set up with the appropriate account and set to remember the master password.
3. Each account would be given access to the logins necessary to that department and the passwords will not be visible except for Sierra.
4. Sierra can be set to remember the password.
5. Changes to logins would happen in the background by the administrator or supervisor.
6. Staff turnover would precipitate a new Sierra password.