PMMI MEMBER PASSWORD AND ACCESS MANAGEMENT CHECKLIST

Have you implemented all of the following controls in your organization?

PASSWORDS

☐ Does your organization publish guidance on passwords and access management to employees?

Does your organization’s password policy require:

☐ Minimum length of 12 – 15 characters?
☐ Complexity including lower and upper case letters, numbers, and symbols?
☐ Expiration at a minimum of once per year?
☐ A certain number of passwords remembered that can not be re-used?
☐ Exclusion of certain familiar words such as company or employee name?

☐ Does your organization encourage the use of pass phrases or “story in a password” that does not contain easily guessed strings? For example: “password” or “123456” or “thisismypassword”

☐ Does your company recommend a particular password vault or safe that employees use?

☐ Does your company train employees not to write down passwords or store them using insecure methods such as text notes or spreadsheets?

☐ Is multi-factor authentication employed to secure access to critical business applications?

☐ Is multi-factor authentication used for all administrative accounts and remote access?

ACCESS MANAGEMENT

☐ Are employees only given access to systems that they need to complete their job responsibilities?

☐ Does your company regularly review access lists to verify the access employees have to corporate systems and to disable idle accounts?

☐ Does your company have a defined onboarding and off-boarding process to ensure the timely addition and removal of access?

ADVANCED CONTROLS

☐ Does your organization employ a centralized identity and access management solution?

☐ Does your organization employ the use of single sign-on to reduce the risk of account breach?