the solutions team Incorporated

TERMINATED EMPLOYEE USER ACCOUNTS

Recently, we observed a situation where a terminated employee attempted to unsuccessfully cause disruption to the access of a client's systems and databases. The safeguards in our systems and our security personnel caught the attempt early in the process before any "damage" was done to any PHI files.

Because of this, we want to reinforce some actions that you must take when any employee leaves your organization; whether by termination or by choice:

1. Immediately disable the terminated employee's access to your systems and computer resources.
   a. You may disable their access by using the Client Administrative Portal (CAP) as shown in the attached instructions.
   b. Or, you may contact The Solutions Team Support Desk and they will disable the terminated employee's access though our available systems.

2. Please send an email to support@mysolutionsteam.com with the following information regarding the terminated employee:
   a. Employee name
   b. Employee user name
   c. Date of termination

This information will help us better secure your valuable databases and systems against any potential reprisals by former employees.

You should verify that any workstation or local device used by the terminated employee is clear from any virus and / or malware infections. If you use TST to manage your local network resources, we will take care of that for you. If you do not use TST for your local network resources, please make sure your local IT company accomplishes this "sweep" as fast as possible.

For any assistance, please contact us at support@mysolutionsteam.com.