

Overview

{COMPANY-NAME} is committed to protecting the privacy of its employees and members and shall protect the confidentiality of nonpublic information consistent with state and federal laws.

{COMPANY-NAME} has an obligation to ensure the security and confidentiality of its member records and to protect these records against unauthorized access that could result in any type of loss or inconvenience for its members.

Purpose

The purpose and principle of a “clean desk” policy is to ensure that confidential data is not exposed to individuals who may pass through the area such as members, service personnel, and thieves. It encourages methodical management of one’s workspace.

Because of the risk of being compromised, confidential information should always be treated with care.

Policy Detail

To maintain the security and privacy of employees' and members' personal information, {COMPANY-NAME} employees should observe the "clean desk" rule. All employees should take appropriate actions to prevent unauthorized persons from having access to member information, applications, or data. Employees are also required to make a conscientious check of their surrounding work environment to ensure that there will be no loss of confidentiality to data media or documents.

The clean desk policy applies to:

- Day Planners and Rolodexes that may contain non-public information
- File cabinets, storage cabinets, and briefcases containing sensitive or confidential information
- Any confidential or sensitive data, including reports, lists, or statements. Sensitive data refers to personal information and restricted data. Personal information includes, but is not limited to:
 - An individual's name
 - Social security number
 - Driver's license number or identification card number
 - Account number, credit or debit card number, security code, access code,
 - or password that could permit access to an individual's financial account
 - Restricted data is divided into two categories:
 - Personal data, that refers to any combination of information that identifies and describes an individual.
 - Limited data, that refers to electronic information whose unauthorized access, modification, or loss could seriously or adversely affect {COMPANY-NAME}, its members, and non-members.
- Electronic devices, including cell phones and PDAs
- Keys used to access sensitive information
- Printouts containing sensitive information
- Data on printers, copy machines, and/or fax machines
- Computer workstations and passwords
- Portable media, such as CD's, disks, or flash drives
- Desks or work areas, including white boards and bookshelves

PurpleSec, LLC

Last Updated: April 30, 2021

Sales@purplesec.us | [Request A Consultation](#)