CMTS|HR

How Does Sensitive or Personally Identifiable Information Leak from Agencies?

Poor employee education and weak processes cause government data leaks, harming employees and leading to public scandals. Reduce your exposure to data leaks by addressing these five issues.

Lack of unified, integrated information management systems – When sensitive employee data is always stored in a secure system, it can be easily managed. But if different employees store data in different places, data will inevitably leak.

Failure to report lost property – If employees who lose property fear punishment, they may delay reporting the loss until it's unavoidable. By this time, an unauthorized party may have had access to the data on this system for days or weeks.

Improperly secured systems – Don't rely on users for proper password management. Require strong passwords and regular password changes. Users should always lock computers when not in front of them and should never allow other people to use their work computer.

Failure to use the "least privilege principle" agency-wide – Users should only have access to the information necessary to complete their job. Unsecured data on network shares increases the amount of data that can be leaked if any one agency employee's password is lost or stolen.

Careless conversations – Conversations are a common source of individual personnel information leakage. Whether employees are in a job interview, a team lunch or enjoying after-dinner drinks, they need to understand the importance of discretion.

http://www.cmtshr.com

1-855-636-5361

A centralized, permissions-based HR investigation system is an essential part of HR information security.