Data management and privacy Most organizations collect, store and process a great deal of sensitive information.If any of this data is publicly exposed or accessible to a competitor or cybercriminal, then the organization may face signi"cant regulatory penalties, damage to consumer relationships and a loss of competitive advantage. Employees within an organization need to be trained on how to properly manage the businesses' sensitive data to protect data security and customer privacy. Important training content includes: The business's data classi"cation strategy and how to identify and protect data at each level Regulatory requirements that could impact an employee's day-to-day operations Approved storage locations for sensitive data on the enterprise network Use a strong password and MFA for accounts with access to sensitive data 2.Clean desk policy Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes.