

Handling Sensitive Information

Mishandling sensitive data can lead to serious security breaches, financial loss, and regulatory penalties. Information such as personal details, payment information, or company trade secrets must always be handled with the highest level of care.



How Risks Arise



Unencrypted Sharing

Sending sensitive files over email or cloud services without encryption can expose them to interception by attackers.

Tip: Always use encryption tools or secure transfer methods when sending sensitive data.



Unsecured Documents

Leaving confidential papers on desks, in unlocked drawers, or visible in public spaces makes them vulnerable to theft or misuse.

Tip: Lock away documents when not in use, even within the office.



Policy Violations

Ignoring or bypassing company data handling policies can create unintentional security gaps. Small mistakes may lead to large-scale leaks or fines under data protection laws.

Tip: Follow company data policies carefully and ask if you are unsure about requirements.



Improper Disposal

Throwing sensitive papers in the waste or deleting files without secure wiping leaves them accessible to attackers.

Tip: Shred physical documents when finished and use secure deletion tools for digital files.