Deloitte Confidentiality & Data Security Fundamentals

Tips and Takeaways

Download and save this PDF to your desktop.

Stay vigilant with the four shields and security tips!

Never send confidential information to your personal email address

Post prudently – Review the Deloitte social media guidelines and applicable contractual obligations.

Keep it professional – Do not send Deloitte, client, or third-party documents to your personal email address.

Keep it in the Deloitte environment – Do not send Deloitte or client files to your personal email address or personal cloud collaboration sites.

Correctly classify data to safeguard information

Don't delay – Reporting the potential incident sooner rather than later is crucial to achieve best outcomes.

Define correctly – Know how to identify the different types of confidential information and personal information for proper data safeguarding.

Use only approved technology

Tech with trust – Only use approved technologies.

Check the plan – Confidential Information Management Plans (CIMPs) establish account team, engagement team, business, and service line strategies for managing confidential information and help to prevent, detect, contain, and mitigate the risk of potential confidentiality incidents.

You can't lose what you don't have

Keep it lean – Schedule time each week to review your inbox and delete messages that are no longer necessary for a business purpose, while noting to retain Official Records and documents under legal holds per your firm's records retention policies.

Archive timely – Properly archive project files, from your laptop or collaboration site within your firm's specified archiving timelines and delete files no longer necessary for a business purpose.

Cut off access – Let collaboration site owners know when you no longer need access.

Security tips

Remain diligent – when working from home, be conscientious about maintaining confidentiality and privacy safeguards.

Do not get phished – Be aware of social engineering attempts and do not click suspicious links in emails.

Don't be anonymous – Keep your security badge visible at all times in the office, even if you are just sitting at your desk.

Report timely – Report potential incidents using your firm's reporting process as soon as you suspect a potential loss or disclosure of any type of confidential information or personal information.

Know your environment – Avoid working on or discussing confidential information in public whenever possible.

No tailgating – Everyone is required to badge-in for themselves at Deloitte and at client sites. Do not allow anyone to follow you through a secure door without a badge, even for people you know.