Deloitte Confidentiality & Data Security Fundamentals

Risk Reminders

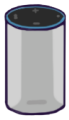
Download and save this PDF to your desktop.

Access Security: Never share your user log in, system credentials, or passwords for any Deloitte or client systems, accounts or devices with anyone – even with team members or clients that have similar access rights. And NEVER write them down anywhere, including on a note that you place on your laptop or within your workspace.

Badge Visibility: While you should always wear your badge visibly whenever you are in the office, you should not display it when out in public as it may make you a target for a data thief.

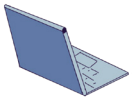
Borrowed Phone Request: Deloitte-issued devices must not be shared internally or externally.

Confidential Information or Personal Data through Text: Never send confidential information or personal data via text message. Text messages can be received by the wrong person if even one digit of the phone number is incorrectly entered. They also have the potential to be intercepted by a malicious third party, screen-captured or forwarded — creating confidentiality, privacy, and cybersecurity risks.



Digital Assistants: Digital assistants in the home may be handy, but they should never be used to record meetings, work conversations, nor even create work to-do lists.

Headphones: Headphones are important to use when working from home if there are others in the household. Using headphones when you take calls or attend online meetings prevents others from overhearing potentially confidential or private information, even if they are in a separate room.



Laptop Privacy: If you must work in public, use a privacy screen and sign onto Deloitte's VPN before accessing any file-sharing sites and before accessing any Deloitte systems, sites, or applications.

Secure Shred: Wastebaskets and recycle bins are fine for ordinary trash, but not for confidential documents. Always use a shredder or deposit documents in a secured shredding bin to destroy hard copies with confidential information once they are no longer needed (as long as they are not subject to legal holds or other retention requirements).

Sensitive Information: It is against Deloitte's confidentiality and privacy practices to leave out sensitive information where others may see it.

Unlocked Laptops: Always lock your laptop using CTRL-ALT-DEL or click the lock icon in the laptop's task bar, and physically secure the laptop if possible, before you leave. Be sure your password is a strong one that is difficult to detect by both humans and computer programs to protect data from unauthorized access by following Deloitte's password protection guidelines.

Unsecured Network: Use secure networks with restricted access (Deloitte, client, and home) and avoid using public wireless.

Working From Home: Working from home poses confidentiality risks. Download the "Working From Home Tips" to learn more.