Confidentiality, Privacy and Cybersecurity

Tips and Resources

Download and save this PDF to your desktop, and open it in Adobe Acrobat to activate the hyperlinks.

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 ensure best outcomes.

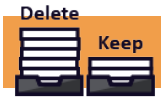
Define correctly – Know how to identify the different types of Confidential Information and Personal Information for proper data safeguarding.

Password protect – Know how and when to encrypt email attachments.

Use only approved technology

Tech with trust – Only use approved technologies. Talk with your team and visit DNet (US/USI) to find "Collaboration Central" and "Approved Survey Tools.

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 – Learn what documents should be retained pursuant to Deloitte records retention policy (APR 601) and what documents should be deleted. Holding onto previous versions of confidential client documents that you no longer need puts you, Deloitte, and our clients at risk.

Keep it clean – Schedule time each week to review your inbox and delete messages, noting to retain Official Records and documents under a legal hold, that are no longer necessary for a business purpose.

Archive timely – Properly archive project files, within firm-approved tools, from your laptop or collaboration site 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 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.

Contact Incident Management – Report online or call 1-800-DELOITTE (US/USI) if you suspect a potential loss or disclosure of confidential information including PII.

Know your environment – Avoid working on or discussing Confidential Information in public whenever possible. If necessary to work in a public place, use privacy screens and VPN to protect confidential information.

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.

Resources

Here are some other resources you may want to note or bookmark for future reference.

Reporting & Questions

- Email – US Confidentiality & Privacy
- Email – Confidentiality & Privacy Incident Management with questions at Incidents (US)
- Self-report on DNet or call 1-800-DELOITTE (US/USI) to report a potential confidentiality or privacy incident
- If you are an Israel Member Firm professional, self-report using the Confidentiality & Privacy incident reporting in ServiceNow at https://deloitteus.service-now.com/israelsp
- If you are a professional in a Member Firm other than US/USI or Israel, follow your Member Firms' reporting processes

References & Policies

- Collaboration Central – US | Global
- Confidentiality & Privacy
- Check if your project is subject to legal holds (US)
- APR 208 Electronic Communications and Systems – US & USI | ISR | GER
- APR 601 Records Retention Policies – US & USI
- APR 910 Privacy Policy – US, USI, & MEX | ISR

Apps

- Can I
- KnowIt