Princípios básicos de confidencialidade e segurança de dados da Deloitte

Lembretes de riscos

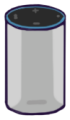
Baixe e salve este PDF na sua área de trabalho.

Segurança de acesso: Nunca compartilhe seu login de usuário, credenciais do sistema ou senhas para qualquer sistema, contas ou dispositivos da Deloitte ou cliente com ninguém – mesmo com membros da equipe ou clientes que tenham direitos de acesso semelhantes. E NUNCA os escreva em qualquer lugar, inclusive em uma nota que você coloca em seu laptop ou na sua área de trabalho.

Visibilidade do crachá: Embora você sempre deva usar seu crachá de forma visível quando estiver no escritório, você não deve exibi-lo quando estiver em público, pois pode torná-lo um alvo para um ladrão de dados.

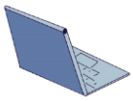
Solicitação de telefone emprestada: Os dispositivos emitidos pela Deloitte não devem ser compartilhados interna ou externamente.

Informações confidenciais ou dados pessoais através de texto: Nunca envie informações confidenciais ou dados pessoais por mensagem de texto. Mensagens de texto podem ser recebidas pela pessoa errada se até mesmo um dígito do número de telefone for inserido incorretamente. Eles também têm o potencial de serem interceptados por terceiros mal-intencionados, capturados na tela ou encaminhados — criando riscos de confidencialidade, privacidade e segurança cibernética.



Assistentes digitais: Os assistentes digitais em casa podem ser úteis, mas nunca devem ser usados para gravar reuniões, conversas de trabalho, nem mesmo criar listas de tarefas pendentes.

Fones de ouvido: Fones de ouvido são importantes para usar ao trabalhar em casa, se houver outras pessoas em casa. O uso de fones de ouvido quando você atende chamadas ou participa de reuniões online evita que outras pessoas ouçam informações potencialmente confidenciais ou privadas, mesmo que estejam em uma sala separada.



Privacidade do laptop: Se você precisar trabalhar em público, use uma tela de privacidade e faça login na VPN da Deloitte antes de acessar qualquer site de compartilhamento de arquivos e antes de acessar qualquer sistema, sites ou aplicativos da Deloitte.

Trituração segura: Cestas de lixo e lixeiras são boas para lixo comum, mas não para documentos confidenciais. Use sempre um triturador ou deposite documentos em uma lixeira segura para destruir cópias impressas com informações confidenciais, uma vez que elas não sejam mais necessárias (desde que não estejam sujeitas a retenções legais ou outros requisitos de retenção).

Informações confidenciais: É contra as práticas de confidencialidade e privacidade da Deloitte deixar informações confidenciais onde outras pessoas possam vê-la.

Classificação: Confidencial – uso interno

Laptops desbloqueados: Sempre bloqueie seu laptop usando CTRL-ALT-DEL ou clique no ícone de bloqueio na barra de tarefas do laptop e proteja fisicamente o laptop, se possível, antes de sair. Certifique-se de que sua senha é forte e difícil de detectar por humanos e programas de computador para proteger os dados contra acesso não autorizado, seguindo as diretrizes de proteção de senhas da Deloitte.

Rede sem segurança: Use redes seguras com acesso restrito (Deloitte, cliente e residencial) e evite usar redes sem fio públicas.

Trabalhar em casa: Trabalhar em casa apresenta riscos de confidencialidade. Baixe o "Working From Home Tips" para saber mais.