Information Security

Protecting Accenture

Safeguarding Accenture: Top Ten Dos and Don'ts

Protecting Accenture's work and confidential client information is everyone's responsibility every day. Here are the top ten Information Security Dos and Don'ts to help you get the job done.

1 Protect your password.

Create a complex and hard-to-guess Enterprise password or passphrase. Immediately change it if you suspect it's been compromised.

2 Use different passwords for personal sites and devices.

Create and use different personal passwords or passphrases for social media and the personal sites you visit and devices you use. Never share your passwords with anyone.

3 Encryption is the key.

If you absolutely have to use external media to transfer data, it must be encrypted. Get an IronKey encrypted flash drive from the Accenture Resource Center or use Bitlocker to Go.

4 Store data properly.

Accenture or client data should never be saved to personal devices or online storage services that are not provided by Accenture. Always use your Accenture PC or an approved and encrypted external device. Only use Accenture's PC back up tool to back up your workstation or laptop.

5 Use data, don't abuse data.

Know the right way to handle sensitive data, and know if you have the right to share client data or deliverables. Limit access to those with a defined business need.

6 Beware of communications from anyone you don't know.

Be suspicious of e-mails, IMs or phone calls from people you don't know requesting Accenture, client or personal information.

7 Beware of people posing as "friends" on social sites.

Be cautious of invitations to social networking sites from people you don't know, and don't post confidential information on social networking sites like Facebook or LinkedIn.

8 Keep your computer secure.

The security tools and settings on your PC are there to protect you and your data. Making unauthorized changes to firewall, encryption or other standard security tools and settings puts you at risk. Contact Technology Support if you think that you have a business need to make changes.

9 Keep your business to yourself.

If you must view sensitive information in public on your laptop, use a privacy screen available from Local Technology Services (LTS), and if you must speak on a phone in a public place, keep your conversation private.

10 If you see something, say something.

Immediately contact the Accenture Security Operations Center (ASOC) at: +1.202.728.0645 if you suspect you have seen or experienced a security incident. Collect calls are accepted 24/7.

Work smart to stay safe. **For more information, visit protecting.accenture.com**