

# Being the Strongest **LINK**

Recognize, Respond to, and Prevent  
Information Security Incidents.



## Do ✓

- Take responsibility for securing the information you create and manage. ◀
- Report known or suspected security issues, such as a computer without antivirus software or a stranger calling and asking for inside information. ◀
- Recognize sensitive information, such as medical, personnel, financial, trade secret, or confidential information, and ensure it is protected. ◀
- Follow our Acceptable Use Policies by limiting your personal use of workplace resources and respecting copyright laws. ◀
- Use secure forms of email when transferring sensitive information over the Internet. ◀
- Use a pass-phrase generated password that is strong and complex, e.g., "Welcome to the 1992 high school varsity reunion." "W2t1992hsvr." ◀
- Report it immediately if your computer lacks antivirus or antispyware software. ◀
- Purchase and use mobile devices with security features such as password protection and encryption. ◀
- Follow our Clear Desk Policy by keeping sensitive information locked away and inaccessible while you are away from your desk. ◀
- Dispose of sensitive information properly, for example, by shredding paper documents with sensitive information. ◀
- Follow all laws, regulations, and policies, including our security policies, which apply to your job function and ask your supervisor when in doubt. ◀

## Don't ✗

- Assume security is someone else's job and not your responsibility. ▶
- Fail to report security incidents for any reason, since without reporting, security issues cannot be resolved and future issues cannot be prevented. ▶
- Share sensitive information with any unauthorized person, discuss it in public places, or store it in unsecured mobile devices. ▶
- Use workplace resources to access inappropriate, sexually explicit, or threatening material or in such a way that interferes with your productivity. ▶
- Transmit medical, financial, trade secret, confidential, or other sensitive information over unencrypted channels. ▶
- Leave your password unchanged for more than 180 days, write it down on a piece of paper, or use easily guessed information, such as your birthday. ▶
- Download and install unapproved software from the Internet, which could contain malware or security holes. ▶
- Place sensitive information on unsecured mobile devices. ▶
- Forget to use a password protected screensaver to ensure no one accesses your computer while you are away from your desk. ▶
- Keep information indefinitely. Instead, follow our Records Retention Policy by disposing of information when its retention period expires. ▶
- Bend or break security rules in order to "simplify" things. Instead, bring positive suggestions to your supervisor on how to securely increase efficiency. ▶



# Travel Safety Best Practices

Please follow these best practices to help ensure your personal safety while traveling.

- Leave a complete itinerary and copies of important documents, like your ID and passport, with someone and check in with that person periodically.
- Ensure your luggage is tagged with your name, address, and phone number and not left unattended.
- Do not transport items for others.
- Be cautious with business gifts received overseas before returning home with them.
- Only use registered taxi services and be sure you are dropped off at a safe, well-lit place.  
Travel with a trusted colleague or companion if possible if in an unfamiliar locale.
- If you are being picked up at the airport, verify the identity of the driver before getting in the car.
- Watch the work you do on places since people may be able to see what you are doing.
- Avoid taking or displaying expensive equipment or jewelry.
- Only take credit cards and money that you need for the trip.
- Do not use hotel business center computers for sensitive data. They can be compromised by cybercriminals.
- Lock expensive items and a backup credit card in your hotel safe.

*This companion document to our security awareness training includes some, but not all of the things you should and should not do to be a **strong link** in the security chain.*