



Privacy Pup's

DATA PRIVACY INSTRUCTION MANUAL

You need to protect your data and the data that you handle at work. But how do you even go about doing that? Privacy Pup is here to help! He is going to walk you through the steps you can take to avoid data privacy leaks.

ALWAYS FOLLOW POLICY!

The advice that follows is intended to be used for general best practices. You should never install or make changes to company property without permission. As always, refer to company policy for more information.



STEP ONE

Install anti-virus and security software.

This is the most important first step in securing your computer and other devices. A device without security software is like a door without a lock; any one could just walk in at anytime.

STEP TWO

Turn on auto-update.

Be sure all your software is set to auto-update, not just your security software. Operating systems and apps have vulnerabilities that are remedied in patches and updates.

STEP THREE

Change your passwords.

Passwords have an expiration date...or, they should. Passwords should be changed often. They should be easy to remember but hard to guess, using a combination of numbers, letters and symbols. Never use the same password for more than one account and never write down or share your passwords.

STEP FOUR

Share less.

Be aware of what you are putting out into the public domain via social media. Manage your security settings so you know who has access to what data about you and your company.

STEP FIVE

Avoid phishing emails.

If it sounds too good to be true, it probably is. Learn to recognize the signs of phishing emails, and who to report them to if necessary. Most important of all, DO NOT CLICK on any link in a phishing email.

STEP SIX

Use a personal VPN on free WiFi.

Free WiFi is potentially very dangerous. To protect yourself from people trying to siphon off your data, you should use a personal VPN on all your devices when browsing on free public WiFi.