The Most Basic OPSEC document: Who, what, when, where, why, and how?

Why: Why bother with OPSEC?
Regulations require an OPSEC program, but the real reason is simple: The more information we give the enemy, the more easily they can damage our mission and kill our people. If we give the enemy less useful information- which we call Critical Information- then they have a harder time planning attacks against us. More difficulty planning for the enemy means fewer enemy attacks, and fewer casualties from the attacks that do happen.

Who: Whose responsibility is OPSEC?
Yours. Whoever you are, whatever job you do, you have Critical Information. The MWR staff member at the gym may know deployment dates because units start canceling scheduled events- but if the enemy knows the deployment dates, they can plan an attack more easily. Everyone has information that the enemy can use to target our missions and our people. It is *your* job to keep *your* Critical Information out of enemy hands.

What: What is OPSEC?
OPSEC is a process of identifying friendly actions that adversaries can observe and interpret to gain Critical Information, then taking steps to reduce the enemy's ability to use that information. OPSEC is avoiding doing things the enemy can watch to determine what's going on and not releasing information that tells the enemy what's going on.

When: When is OPSEC important?
Constantly. Even when we're just doing our normal operations, we are showing the enemy how we work. We train like we fight, so the enemy watches us train. When we're returning from the field, the enemy watches us for lessons learned. We're being observed all the time, so we have to use good OPSEC all the time, too.

Where: Where is OPSEC applicable?
Everywhere. OPSEC applies to troops in the field, no doubt. It also applies at stations where units are getting ready to deploy, posts where forces are returning after deployment, and to bases where support entities that never deploy are assigned. It's easy to forget OPSEC when we're home, but the enemy observes us everywhere, not just overseas, so we have to employ good OPSEC everywhere, as well.

How: How do I improve my personal OPSEC?
First: Know your Critical Information. Talk to you r unit OPSEC officer to get a Critical Information list. Generally, the enemy wants to know about capabilities, activities, limitations, and intentions- so those are items to protect.
Second: Prevent giving away Critical Information. Don't put Critical Information in non-secure email, or talk about it in non-secure telephone calls, if possible. Don't post Critical Information to the web. If you post about what you did that day, you may be describing tactics. You may only intend to send your family a picture of yourself at work, but that may show sensitive equipment or a site that the enemy can target.
Bottom line: Look over the information you put out; consider if the enemy can use any of it; and if so, then don't release it without proper precautions.