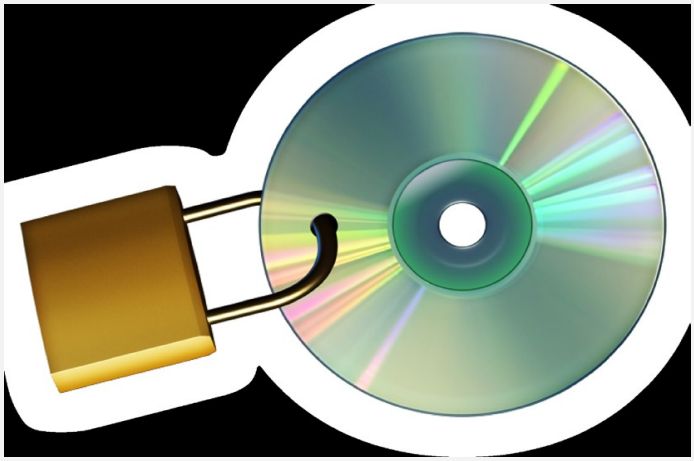
your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Data Security

Problem
A great deal of our security focuses on keeping our devices, such as firewalls, anti-virus, and system updates, secure.. While these are important, ultimately, most attackers are not after our organization's computers or devices, but the information residing on them. We have a tremendous amount of sensitive information that must be protected at all times.

Solution
Technology can only do one part in protecting our data. We depend on you to protect our organizations sensitive information. To ensure our data always remains secure, you are required to take the following steps whenever handling any sensitive information:



Data Protection
Our information is our greatest asset; it is also the primary target for many cyber attackers. Technology alone cannot protect our highly valuable data; we need your help. It is critical you follow the steps provided to help protect our sensitive information.

- Always understand the sensitivity of the information you are working with. If you are uncertain about the sensitivity of any information or the steps you should take to secure it, ask your supervisor.
- Use only systems authorized by our organization to enter, process or store sensitive information. Do not copy or store sensitive information to any unauthorized systems or accounts, such as personal laptops or personal email accounts like Gmail or Yahoo.
- If you transfer sensitive information, use secure, authorized methods that support encryption. Do not transfer sensitive data using insecure means, such as email, unless you are using specialized encryption software that you have been properly trained to use.
- You must have prior approval to store sensitive information on removable media or portable storage systems, such as CDs, DVDs, USB flash drives and external hard drives, which should be encrypted using approved encryption software.
- Never store or share sensitive information on public Internet or Cloud services such as Dropbox, Apple iCloud or Google Drive unless you have prior authorization from management.
- Be careful responding to any emails or phone calls in which someone is asking you to send them sensitive information. Always authenticate the person first using approved procedures, then ensure they have authorization to access such information.

- Any sensitive information should be backed up on a regular basis using approved procedures, so if the device is lost, stolen or its data is corrupted, you can recover the data. In addition, remember that backups can also be a target and should be properly secured, including the use of encryption.
- Never leave any sensitive documents unattended at your desk. Instead, secure sensitive documents when you leave them, such as locking them in a secure cabinet. In addition, whenever you leave your computer, make sure the screen is password protected. This ensures that no unauthorized personnel can walk up to your computer and access your confidential information while you are away.
- Never leave any sensitive documents at printers or fax machines; be sure to pick the sensitive documents up as soon as they are ready.
- Use only authorized software for work-related activities; never install or use unlicensed or unauthorized software.
- Any sensitive information that is no longer necessary or appropriate to store should be properly destroyed, shredded or rendered unreadable.
- If you believe any sensitive data has been lost, stolen or compromised, be sure to contact the help desk or security team immediately. The sooner our organization is notified the more likely it is we can safely recover from the incident.

By following these steps, you help ensure both our information and our organization remains secure.

Advanced Threats After Our Data

There are many different threats targeting our sensitive data. One of the most common is cyber criminals. These are individuals or organizations who know they can steal our sensitive data and use it to commit fraud or simply sell it to other cyber criminals. Unfortunately, there are several other threats targeting our sensitive data -- threats even more advanced than common cyber criminals.

One is our competitors. Some of our competitors may be very unethical in the ways they operate. They may try to compromise our organization to gain a competitive advantage, and to do so they need our data.

Another threat is other countries. There are certain countries that target our data for economic, political or military gain. Individuals launching these attacks are often supported by their government, and it is many times part of their full-time job. You may not think our data has value to other countries, but it does.

This newsletter is published by OPPD's

Cyber Security & Information Protection Department.

For more information, please contact us at:

IT-ServiceDesk@oppd.com

your energy partner®
OPPD
Omaha Public Power District