Information Security in the Workplace

A GUIDE

COURTESY OF ERMProtect
Cybersecurity Solutions

ERMProtect
Cybersecurity Solutions

Cyber & Information Security is Everyone's Responsibility

You Can Make a Difference!

Companies must consider information security and data protection to be of paramount importance and an essential cornerstone of their operations. Every employee must be responsible for securing the company's information. Vigilance, awareness and good security and data protection practices are the most effective means we have of providing this protection.

The guidelines in this booklet are intended to give employees basic information to help safeguard them from situations that could put a company at risk. These represent a limited sample of information security practices, and should be supplemented and customized by your Information Security Department to address the complexity or your organization's data environment and applicable legal requirements.

If you have any questions regarding information security, please contact us at ERMProtect, where our mission is to protect individuals and organizations from data breaches.

About ERMProtect

ERMProtect is a leading Information Security & Training Company in Miami, Florida. We identify IT vulnerabilities, secure systems, and train employees to recognize when they are being targeted by hackers. Founded in 1998, the company has served more than 300 clients globally in over 25 industries.

Access Controls

Allow Only Appropriate Access to Company Information

Access to sensitive or proprietary information is often provided as part of your job duties. Because of this access, everyone plays a significant role in protecting company information from damage, loss, misuse or unauthorized disclosure.

It is particularly important to ensure the security of any regulated data, e.g. personal identifiable information (PII), personal health information (PHI) and payment card information (PCI).

Fines are common for misuse of this information.

Effective May 25, 2018 the new EU General Data Protection Regulation (GDPR) became effective and a company can be fined 4% of annual global revenue or €20 million whichever is greater for misuse of information of EU citizens without prior consent. No personal data can be disseminated to third parties for purposes other than the purposes for which they are collected.

We are all responsible for making sure that only authorized users can access company information.

- Restrict access on a "need-to-know" basis — access to information should only be provided where there is an established business need.
- Ensure that all devices connected to your PC are approved by the Information Technology Department.
- Lock or logoff computers when away from your desk (**CTRL-ALT-DEL**, then lock workstation or logoff).
- Access to systems and company facilities must be removed as soon as employment or a contractual relationship is concluded.
- Report all lost or stolen access cards, laptops or phones to the IT Support team.

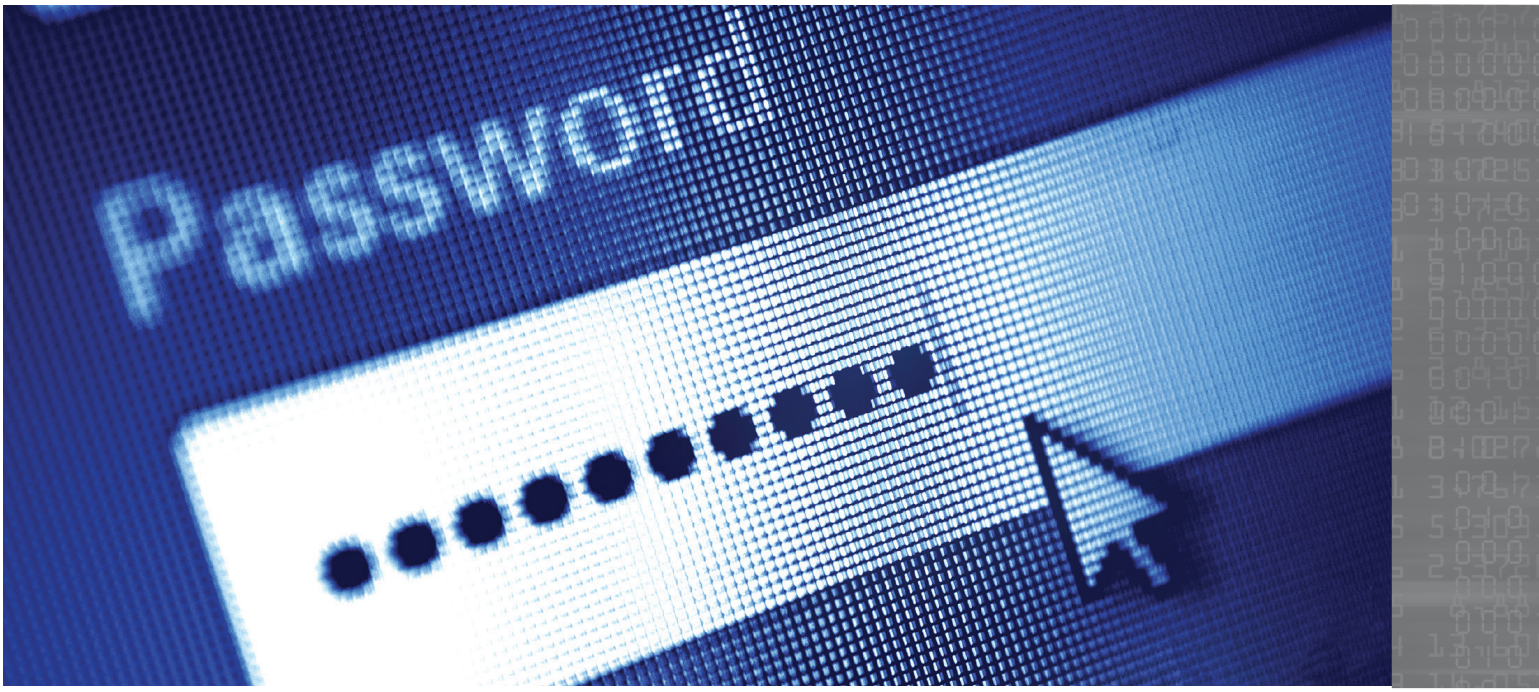
Passwords

Keep Your User-ID, Passwords and PINs Confidential

To access company information systems a user-ID and password is required. This ensures that only authorized access to company's systems and data is allowed and can be reliably tracked. Everyone has been assigned his or her own individual user-ID with a unique password for system access.

Keep in mind the following ideas to help keep your password confidential:

- Be creative and careful when selecting a password. Don't use anything that can be easily guessed, including personal information (such as names, hobbies, or other information about one's self that can be readily discovered) or commonly used words.
- Passwords should be at least ten (10) alphanumeric characters in length. They should contain a combination of letters, numbers and symbols. One technique for selecting and remembering a password is to pick a phrase you find significant. Construct a password using any letter from each of the words in the phrase.
- Passwords should be changed at least every 90 days or whenever you believe their confidentiality has been compromised. You can change an existing password at any time. For example, with Windows, press **CTR-ALT-DEL** keys simultaneously and then select Change Password.
- Passwords should not be shared, posted, written down, reused, revealed to anyone, or used externally to company (for example, Internet accounts).
- Do not include passwords in an automated logon process (for example, do not store a password in a macro, logon script or function key).
- Passwords should also be used on laptops and mobile devices (e.g., mobile phones, laptops and iPads) to protect the information on these devices.
- **Protect your password! You are responsible for all actions taken with your user-ID.**



ERMProtect
Cybersecurity Solutions

Physical Security

Protect Your PC From Theft and Unauthorized Use

Computers are valuable; they contain expensive components, software and most importantly, data. Good physical security practices include:

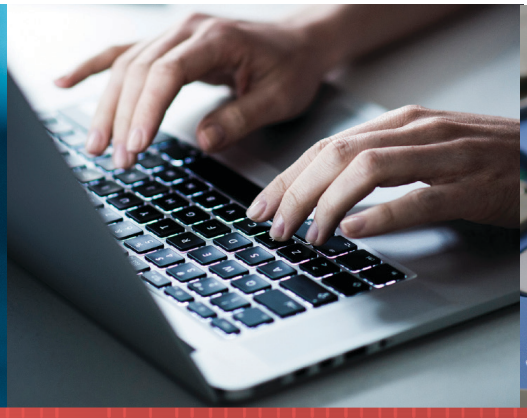
- Restrict physical access to machines. Know who uses or services your computer. Only provide access to trusted and authorized individuals.
- Never leave a laptop unattended without securing it. When traveling, keep it with you and in sight always.
- Do not allow an unknown person to pass through secured entrances (e.g., tailgating behind you). All visitors must show identification prior to gaining access to restricted areas. Advise individuals without appropriate authorization to go to the visitor reception area.
- Make sure that visitors are always escorted by an authorized employee, consultant or contractor. Question any strangers in your work area.

Removable Media Security

Ensure Protection Over Information on Removable Media

Removable media (e.g., CDs, hard drives, USB drives and other media) can contain critical information that must be properly secured. Therefore, the following best practices should be followed:

- Lock up removable media containing sensitive or proprietary information when not in use.
- Do not place removable media near magnets, or other magnetic devices, as they could destroy information.
- Properly label removable media.
- Do not dispose of removable media that contains company data without ensuring the destruction of that information (the delete command by itself does not permanently erase files; the information can still be restored).


Computer Viruses

Prevent Viruses — Being Alert Is Our Most Important Defense

Computer viruses can severely impact your ability to use your computer and can put your files and programs at risk. Furthermore, viruses can easily spread throughout the network, usually without any intentional action on the part of the victim. Virus outbreaks can have a significant impact on the network and could cause damage or loss of valuable information. You can prevent virus infections by following these procedures:

- Never open an unexpected e-mail attachment. Also, make sure that the source and purpose of any attachment is understood before opening. E-mail can be forged and malware can automatically proliferate.
- When in doubt, you should verify the contents of any attachment with the actual sender before opening it.
- Do not allow files to execute macro commands without understanding what they do and where they originated. Macro commands can propagate malware and may be embedded in Microsoft Office files (e.g., Word and Excel) and other data files. You can usually use these files successfully and without risk by simply not permitting macro commands to run when such files are opened.
- Avoid sharing or using software, CDs and files from unauthorized sources.
- Make sure that your computers, especially laptop and home PCs, are always running current patches and anti-virus software with routine virus prevention updates (update it on at least a weekly basis).
- **Be suspicious of irregular system behavior and report it to IT Support**

ERMProtect
Cybersecurity Solutions

Software Piracy and Copyright Laws

Use Only Company Licensed Software on Your PC and Macs

Do not install any software on your PC or Macs without direction from Information Technology. If you have a requirement for specific software (especially Internet downloads or additional business software), please ask the company for guidance.

Creating unauthorized copies of vendor software can result in serious legal complications. If employees use illegal copies of software, the company and employees may face civil and criminal liability. Furthermore, unapproved software may not work correctly on company computer systems, and may cause system malfunctions, inoperability and potential file loss. For these reasons, use of unauthorized software (including screensavers and utility programs) is prohibited.

If you are using unauthorized copies of software, please remove them from your computer immediately.

E-Mail Usage

Use Care When Sending E-Mail

E-mail is inherently insecure unless you take special precautions. All your messages go through multiple machines before they finally end up at the right destination. Once sent, you no longer have control of distribution and there is no assurance of a message's authenticity. You can do some simple things to lessen these risks:

- Be cautious about what you send. Unless encrypted, you should assume that someone other than the intended recipient can read your mail. You also do not know where your message may be forwarded.
- Be wary about the actual source of received e-mails. E-mail can be forged, so you should consider this fact always and treat each e-mail cautiously. Be especially careful when opening an attachment. It might contain a virus.
- Before replying to an e-mail, check distribution. Be particularly careful when using the "Reply All" feature. This can result in the proliferation of numerous messages, and may adversely impact the entire e-mail system.
- A company e-mail system is provided for business purposes. E-mail messages should reflect the professional content and quality of a written document. Any solicitation and distribution of nonbusiness related material (e.g., advertisements, chain letters, and offensive language) is not permitted.
- Do not access your non-company e-mail accounts (e.g., Google, Yahoo or Hotmail) from your work computer.
- **Remember that the e-mail system provides no assurance of privacy.**

Using the Internet

What are the Risks?

The Internet is an extraordinary resource, but it is also an unregulated environment. Internet access is provided to assist you in performing your assigned job duties. You are expected to use this access in a professional and responsible manner.

To get the most from the Internet without exposing a company to unnecessary risks, you should be attentive to the following:

- When viewing or requesting web content, programs may be automatically initiated. Do not choose to execute such programs without being sure of their source, their function and their effect on your machine's operation. It is always best to check with IT Support when in doubt.
- Your Internet activities may occasionally cause security warnings to appear. Pay attention to these messages and act cautiously. If you are unsure about how to proceed, contact IT Support.
- Don't assume that information found on the Internet is necessarily accurate or up-to-date.
- Make sure that all materials you download comply with all applicable laws and copyright restrictions.
- Unless you have proper authorization, do not share any information that is proprietary to the company or purports to represent the company's views in any way.

As a rule, companies regularly monitor the usage of their Internet systems.

ERMProtect
Cybersecurity Solutions

Mobile Devices

Security Tips for Mobile Devices

Mobile devices are a convenient way to take information and databases anywhere you go. Unfortunately, their portability makes them a popular target for thieves. Sensitive information is often maintained within mobile devices such as laptops, mobile phones and handhelds (e.g., iPhones, iPads, PCs and Macs). The following tips will assist you in safeguarding mobile devices, as well as the sensitive and proprietary information they may contain:

Do's ...

- Backup your data regularly and keep a current copy in a separate location.
- Keep mobile devices out of sight and secure whenever possible.
- Know what you have stored on your devices and periodically inventory their content.
- Require passwords for all access to your mobile devices.

... and Don'ts

- Don't store sensitive information (e.g., your password, credit card or telephone card data) in devices. Such devices often have limited security and are usually unable to withstand a determined attack.
- Don't leave a mobile device unattended. Mobile devices are easily lost or stolen. When traveling, carry the device as hand luggage and be cautious in public places (e.g., airports or hotels).
- Don't discuss or view sensitive or proprietary information where others may be able to hear or view the information.

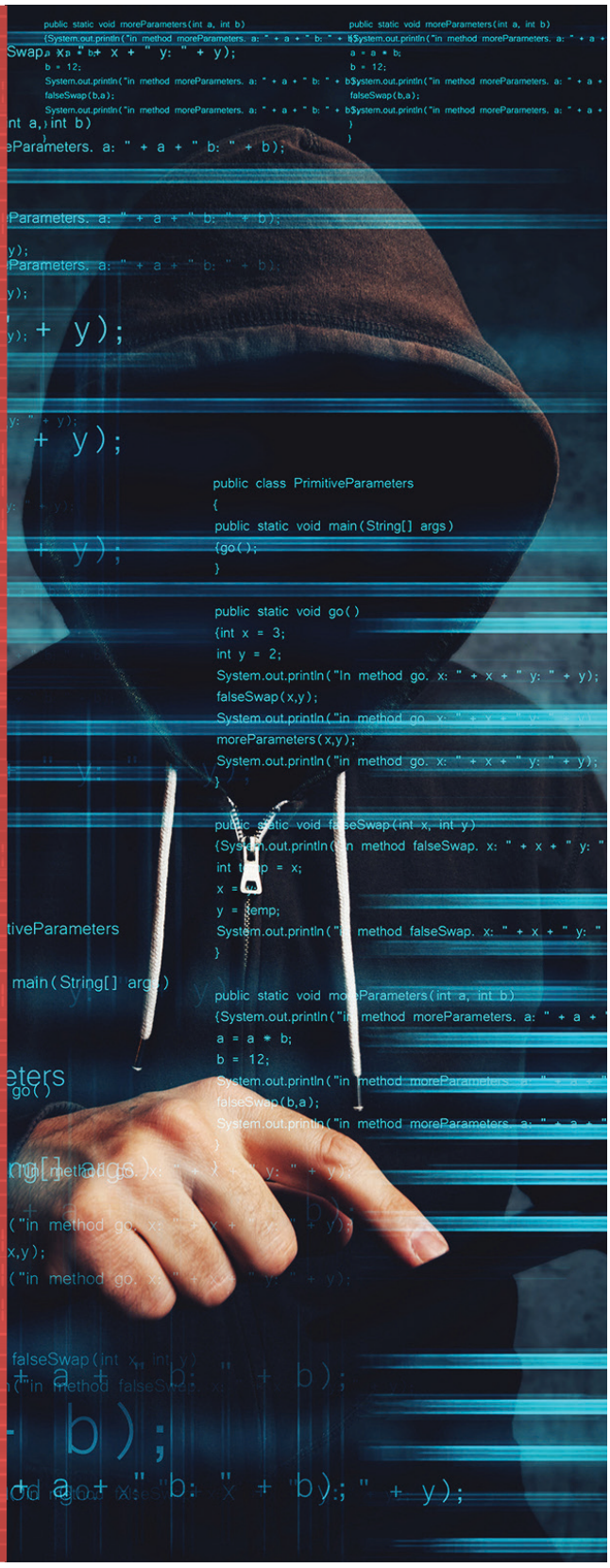
Handling of Sensitive or Proprietary Information

Secure Sensitive or Proprietary Information at All Times

All company information should be protected to the degree suitable to its contents. Information that is especially sensitive to unauthorized disclosure will need to be especially well–protected.

- Clearly identify and label sensitive or proprietary information. Make sure all such information is securely filed and put away when not in use.
- Lock desk drawers, cabinets and file rooms that contain sensitive or proprietary information.
- Make sure that access to sensitive or proprietary data is limited only to authorized individuals. Review the list of who has access and periodically confirm that this remains appropriate (IT Support can assist you in doing this).
- Properly dispose of company information when it is no longer needed. Shred sensitive or proprietary information after usage (subject to legal and regulatory requirements) or put in secure bins.
- Do not send sensitive or proprietary information via computer unless it is encrypted or password-protected. Company IT Support can assist you in establishing encryption capabilities.
- Only access, copy, modify or disclose information as needed in fulfilling your job responsibilities.
- Promptly collect sensitive or proprietary documents when printed. Don't print sensitive documents on remote printers in unsecured areas.
- Sensitive or proprietary information should never be sent to an unattended fax machine. Call ahead to alert the receiver.
- Upon leaving the company, you should return all sensitive or proprietary information in your possession to your manager.

ERMProtect
Cybersecurity Solutions



Anti-Hacker Checklist

Never Divulge Information to Strangers

Many hackers obtain sensitive or proprietary information by contacting employees who unintentionally respond thinking that they are being helpful. Here are some tips that can help minimize the potential for unauthorized access to sensitive or proprietary information:

- Verify the identity of callers requesting information. If you can't immediately identify them, insist on calling them back. You should make sure that they are legitimately entitled to receive any information being requested.
- Don't give out information about yourself or other employees. Refer all inquiries to Human Resources. See your manager if you have any questions.
- Don't discuss company computer hardware, software or environment (including network connectivity) unless you know the person or can verify both his/her identity and his/her need to know.
- Care about your customers, but be aware. Don't let yourself be pressured or manipulated. When someone calls asking for your help in some way that is unusual, be cautious and purposeful in your reaction.
- **Never under any circumstances give out your password to anyone, no matter how urgent the request.**

If you believe that you received an inappropriate request for information, report the incident immediately to your manager, IT Support and/or the Information Security team.

Beware of Phishing

Be on the Lookout for Common Hacker Lures

Computer users are likely to receive spoofed emails (also known as phishing emails) that appear to be from a reputable organization such as a bank, asking for personal details, passwords, credit card numbers, etc. Here are some things that are typical in a phishing message:

- A general greeting such as "Dear Bank Customer" or "Dear Email User."
- A forged or strange email address in the "From" field.
- A threat that something bad will happen if you don't act immediately e.g. your bank account will be closed.
- A link that looks legit but takes you to a malicious site. (Hover over the link to see where it is really taking you.)
- Misspellings, incorrect grammar, and odd phrasing.
- A URL that begins with http://. Only enter personal information on sites that begin with https://. The "s" stands for secure.

Appropriate Usage of Technology and Monitoring

Comply with Laws, Regulations, Policy and Contractual Terms

Company information resources are provided for business purposes. Use technology in accordance with the company's Information Security Policy.

The company owns all its computer assets, including e-mail, Internet access, data, documents and software residing on its systems. The company reserves the right to access and monitor this information.

ERMProtect
Cybersecurity Solutions

800 S. Douglas Road, North Tower, Suite 940
Coral Gables, FL 33134
Phone 305.447.6750
info@ermprotect.com