**1. EPAM Information Security Program**

**1.1          Agenda**

In the current tutorial, we will

* Introduce you to the objectives of the EPAM Information Security Program.
* Define IT Security.
* Explain your responsibility and sources where you could get help regarding security issues.
  + What precautionary measures you have to take in order to avoid becoming a victim of spoofing /credential harvesting attack.
  + You will understand the most common and less-common Customer side exploitations that a malicious hacker might utilize in order to gain access to your computer.
  + You will learn threats related to your mobile communication.
  + You will understand what the warning signs of different attacks are.
  + You will understand the importance of the security for your home computer.
  + You will understand how the improper usage of your browser may lead to a security breach.
* Review the existing precautions against computer incidents and speak about security requirements.
* We will also look at the Labor Safety and Fire Prevention training material.

**1.2          Importance of Security**

**Shift in Perception – Be Security Conscious**

Security is just as strong as its weakest link, and the human factor is the weakest link in information security as in many cases the leakage could have been avoided if the person involved had better knowledge of data protection. An inadvertent action is enough to compromise the security of your computer and ultimately jeopardize the whole IT infrastructure of EPAM. Therefore, you are recommended to develop an information security mindset, building and reinforcing good practice through regular updates of information security awareness.

**Security is critically important.**

* Change Your Perception: Security is a necessity - not a burden.
* Be a Learner: Understand security threats and vulnerabilities. Be aware of the various types of Customer side exploitation.
* Be Proactive: Everything can depend on your security awareness. Make sure you can avoid XSS and CSRF attacks.
* Seek Help and Advice: Advanced technologies require educated users. As a security conscious IT professional make sure you understand what threats may be lurking at you from all angles in the wild.
* Computer Security has utmost importance. We at EPAM do coding and consequently deal with information which others may want to obtain.

**1.3          Objectives of the Security Program**

**Objectives of the EPAM information security program:**

* Identify the goals of IT security.
* Learn about your responsibilities and where to get help when you need computer assistance, or when you experience security problems.
* Learn how EPAM protects its IT resources from attacks and intrusions.
* Find out where you can get more training.

**1.4          Defining IT Security**

Safeguard measures are put in place to help minimize vulnerabilities and to ward off threats.

IT security is about protecting information assets by effectively managing risks. How much protection depends on the risk and magnitude of harm that could result if the data were lost, misused, disclosed or modified.

**Assets** are computers and data.

**Risks** are managed by evaluating:

* Vulnerabilities
* Threats

**Vulnerabilities**

Vulnerabilities are weaknesses in a computer or network that leave it susceptible to potential exploitation such as unauthorized use or access. Vulnerabilities include but are not limited to weaknesses in security procedures, administrative or internal controls, or physical configuration; or features or bugs that enable an attacker to bypass security measures.

**Threats**

Threats can be categorized as such:

* A person (careless oversight, lack of training, malicious or criminal intent)
* A thing (a faulty piece of equipment)
* An event (a power outage, fire or flood)
* Direct attack - attacks on layer 2 (Network)
* Customer Side attack – by sending malicious attachments to the victim
* Company espionage
* Several forms of Social Engineering:
  + Phone calls trying to persuade the victims to give out their password
  + Emails with “instructions” to install programs
  + Links to “sites”

A threat is the means through which a weakness can be exploited to adversely affect a network or supported systems. A threat is possible only because the system is vulnerable to that particular threat.

**1.5          Computer Security Encompasses**

The EPAM IT Security department is responsible for ensuring the security of EPAM information resources.

**Confidentiality:** Confidential information is protected from unauthorized disclosure.

**Availability:** Automated systems are available when needed.

**Integrity:** Electronic information is not corrupted. Integrity also includes:

* Authenticity: The ability to verify that content has not changed.
* Non-repudiation: The origin and receipt of a message can be verified.
* Accountability: The actions of a person can be traced to that individual.

**1.6          What Is Your Responsibility?**

Senior managers and supervisors are responsible for exercising security in their day-to-day operations.

You are responsible for your computer and the information on it. You are to conduct yourself in an ethical manner.

Users must:

* Follow the technical, personnel, administrative, and telecommunication safeguard for computer systems you use.
* Follow the Customer’s security policies and requirements including the related rules as defined by the Customer.
* Undergo user awareness training annually.
* Report computer incidents or any incidents of suspected fraud, waste, or misuse to Support Team (as a new request to [SUPPORT.EPAM.COM](https://support.epam.com/)) or IT Security Team.

Unauthorized computer programs may contain malware. Always use firewall and antivirus solutions.

At home, make sure that you are using your computer behind a router in the Internet connection.

**1.6.1     Safeguards**

Safeguards may include special requirements for:

* Passwords
* Restrictions on access
* Encryption
* Antivirus solution
* Firewall
* In case of home Internet connection, use of a router is strongly recommended.

Home routers are affordable and can act as an intermediary defense layer.

**1.7          Where to Get Help?**

Computer incidents include compromised systems, attacks made on or from EPAM computers, illegal or inappropriate use, and abuse of computer privileges.

What happens when something goes wrong with your computer? Is it a security problem or a technical problem?

Your major sources of help are:

* EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)): for technical and security problems, theft of equipment, and for reporting incidents of suspected computer fraud, waste or misuse
* IT Security Department (ITSD): security engineers to assist you with security policies, issues and problems

**Examples of Computer Incidents**

You receive a PDF file. When you open it, it goes blank and you are staring at a white page.

By now a session has been established to the attacker. Unplug your computer immediately from the network, because every second counts. If you can’t unplug your computer from the network in less than one minute, the likelihood of being ‘backdoored’ increases significantly.

You realize that your antivirus program has been turned off by itself, you turn it back on, but it turns off again. This is a sign that your computer has been compromised already.

You receive a link to a domain that you may or you may not know. The sender encourages you to open it. When you open it, you get redirected to a site and at the same time you may see other EPAM sites, e.g. OWA open either in the back-tab or in the main browser, which asks you to log in.

The sites which may open could be various, e.g. FACEBOOK or GMAIL. The typical message is ’login session expired please re-login.’ If you type your password, you will be redirected to the real site, but by now the attacker has your credentials.

ALWAYS LOOK at the ADDRESS field of your browser. Your attacker's IP address will be there. (It may be converted into a hexadecimal form.)

**Example of a Mobile Security Incident**

You receive an email asking you to install a new ‘Profile’ to your mobile phone.

* Contact to EPAM Support Team promptly. Verify the authenticity of the message.
* Make sure your case has been escalated.
* You think someone is using a computer without authorization.
* Your files look like someone has been tampering with the data.
* Confidential information has been disclosed.
* Your computer is acting strange.

Additional examples include: hacker attacks, suspected fraud, waste, or abuse of a system, web page defacement, inappropriate use, improper disclosure of confidential information, inability to access your files, and theft of data (including disks).

Report any case of theft to the **EPAM Support Team (**[**SUPPORT.EPAM.COM**](https://support.epam.com/)**)**. Users should also contact their local property representative for hardware theft and their IT Security Department for hardware and data theft.

**Types of Information to Be Reported**

Report all aspects of the problem, for example:

* Any suspicious computer messages (e.g., you have received malware and/or other threats).
* What you were doing when the problem occurred.
* Details on how your computer is acting.
* Whether others are affected by the problem.
* Whether confidential information is involved.

**Help Request Processing**

Support Team is available 24x7.

Requests to Support Team ([SUPPORT.EPAM.COM](https://support.epam.com)) can be submitted in the following ways (listed in the order of preference):

* Via EPAM Service Portal: <https://support.epam.com>
* By email to [support@epam.com](mailto:help_desk@epam.com).
* By Belarus phone: +375 17 389 0100 ext. 50911
* By China phone: +86 755 86209999 ext. 50911
* By Hong Kong phone: +852 3757 9428 ext. 50911
* By Hungary phone: +36 1 327 7400 ext. 50911
* By Kazakhstan phone: +7 7172 475 970 ext. 50911
* By Russia phone: +7 495 730 6362 ext. 50911
* By Ukraine phone: +380 44 390 5457 ext. 50911
* By US phone +1 267 759 9000 ext. 50911
* EPAM locations phones: [www.epam.com/contact](http://www.epam.com/contact)
* By email to IT Services Security Team: [WFTITServicesSecurity**@**epam**.**com](mailto:WFTITServicesSecurity@epam.com)

**1.8          On the Lookout for Incidents**

EPAM monitors the security of the EPAM network 24 hours a day, every day of the year, through automated security processes.

A specialized group of experts, the Incident Response Team (IRT), is the focal point for computer security incidents. They provide immediate diagnostic and corrective actions to prevent the loss of EPAM information.

**Intrusion Detection Software**

This specialized software operates at the connection between EPAM network and the Internet. It allows the IRT to monitor network traffic for activity that suggests an attack attempt and helps to identify systems or data that could be exploited. The IRT can then advise about the need for installing software patches (fixes for problems), reloading operating systems, or reconfiguring systems.

**Firewall**

Firewalls are like gateways that allow us to filter out and block certain types of Internet traffic. By setting up special security rules, we can proactively block specific viruses, Internet worms, incident types and known or suspected hacker locations.

**Vulnerability Scanning**

This automated network-scanning tool identifies vulnerabilities or misconfigurations of systems connected to the EPAM network that hackers might use to attempt unauthorized access to systems. The IRT sends this information back to the appropriate organizational entity so that they can address the problem.

**Antivirus Software**

EPAM uses antivirus software on its main firewall to detect and block incoming Internet virus attacks. This software is in addition to the antivirus protection installed on our email servers and desktop workstations.

**1.9          Different Remedies for Incidents**

Incidents have different remedies:

* The EPAM firewall can filter and block certain types of Internet traffic from EPAM IT systems.
* Security scans of systems connected to the EPAM network can detect known vulnerabilities. Institutes and centers get the scan results and advise on corrective remedies.
* Antivirus software may require an upgrade of the EPAM firewall, email servers, and/or desktop computers.
* Based on intrusion detection findings, advisories are sent out to EPAM IT staff about the need to install software patches or other corrective actions.

**1.10         Planning Ahead for Security**

Security requirements are based on the sensitivity of the data and how critical the system is to the EPAM mission.

Risk assessments are performed on critical EPAM IT systems to identify potential vulnerabilities and recommended safeguards.

Using this information, individual security plans are developed to define what measures (controls) are necessary to meet the security requirements.

**1.11         Look Out to Labor Safety and Fire Prevention**

**Labor Safety and Fire Prevention** aspects must be taken into account when dealing with IT Security. The work environment must be set up and maintained, and all employees must work according to the related rules and regulations.

Please complete the EPAM Labor Safety and Fire Prevention training material at [EPAM Labor Safety and Fire Prevention Training](https://kb.epam.com/display/EPMKPAL/Labor+Safety+++and+++Fire+Prevention+Training)

Then, use the check box and button below to confirm that you have understood it, agree with its content, and are ready to work accordingly.

# 2. Using IT Resources

## 2.1          Agenda

The current tutorial will introduce you to the rules of IT Resources usage.

## 2.2          Objectives

The objectives of this section are as follows:

* Understand the responsibilities that accompany the use of Corporate IT resources.
* Learn where to access EPAM policies and guidance that address appropriate use.
* Learn about the proper use of the Internet and email, and about the proper personal use of your computer.

## 2.3          Rules of Conduct

**The rules exist because:**

* Security conscious users are the foundation of a successful security program.
* People function best when they know their responsibilities and boundaries.

Have you seen any of the following inappropriate behaviors?

* Summer student: An employee is caught downloading music from the Internet and copy it to his/her own MP3 player/Pendrive.
* Contractor: Seemingly "unaware" that he was accountable to the same standards as EPAM employees, a contractor uses his EPAM Internet access to download pornography.
* Budget analyst: As the president of her investment club, the budget analyst used her EPAM email account for sending out correspondence and newsletters to all club members
* Scientist's child: The software developer's "whiz kid" son uses his dad's EPAM home computer, hacks into his high school's academic database, and changes grades for his friends

**PAL**

EPAM Information Security Management System's documentation including policies, processes, work instructions and guidelines, can be found in the Process Asset Library (PAL): <https://pal.epam.com>

Concerning the actual policy updates, please visit the [related KB page](https://kb.epam.com/display/EPMKPAL/PAL%3A+What%27s+New) maintained by the QA Team.

All EPAM users must read - and agree to follow - EPAM Policies.

**Important:** Continuing this course constitutes your acknowledgment that you have read and agreed to follow EPAM Policies.

### ****2.3.1 Working at Customer premises****

EPAM employees working onsite, i.e., at Customer premises, must follow the policies, processes, work instructions and guidelines of the Customer.  When non-contradicting overlaps with EPAM policies are recognized, you should follow the more rigorous one. For example, it is recommended to use Kensington lock to protect your laptop even if it is not requested by Customer policies.

If you are not aware of the Customer's policies, immediately ask your Account Manager or Project Manager for a training request.

The main compliancy rules for EPAM employees accessing Customer Data:

* Enter and leave Customer buildings only at the approved entry and exit points and within normal working hours. If you need access significantly outside normal working hours, there should be a justifiable reason. Check with EPAM Data Protection Officer and/or EPAM Account Manager if in doubt.
* Do not bring guests into the Customer building without explicit written Customer approval.
* Do not leave an RSA token or Customer entry badge unattended in any public place. In particular do not leave it visible and unattended. Do not attach any information to the RSA token identifying it with the Customer.
* Do not leave any portable device unattended in any public place where it may be lost or stolen. Laptop hard disks must be secured and encrypted. EPAM applies automatic process to encrypt EPAM laptops with BitLocker.
* Do not use a private laptop for work, do not under any circumstances store any Customer-related data including documents and emails on a private laptop, do not connect it to EPAM and Customer systems and applications. If this prevents effective working, contact the EPAM Account Manager.
* EPAM employees working outside the Customer office must not leave visible any unmasked Personally Identifiable Data.
* EPAM employees should never attempt to access, and not allow access to, Customer Data to which they are not entitled or do not require for providing the Services (i.e. deliver the project)
* EPAM employees shall never use Customer Data for any purpose other than that of providing the Services (i.e. deliver the project)
* Customer data cannot be disclosed, sold, assigned, leased or otherwise disposed of to third parties
* EPAM employees should not store or access Customer data from locations outside the locations/offices contracted.
* Do not transmit any Customer code outside the Customer network, by email or any other means. If an exception is needed in order to perform the contracted duties, it must be agreed in advance with the EPAM Data Protection Officer, EPAM Account Manager and the responsible line manager at Customer.
* Other than where explicitly agreed, it is forbidden to hold any Customer unmasked Personally Identifiable Data – e.g. name, email address, phone number etc., - report immediately to EPAM Data Protection Officer and/or EPAM Account Manager, as this contravenes our agreements with the Customer.
* EPAM employees are under EPAM’s Non-Disclosure Agreement with Customer. Do not discuss any aspect of your tasks with anyone outside EPAM/Customer, and even with EPAM/Customer staff share information only on a need-to-know basis.
* The following may be considered to be a security incident (until otherwise clearly stated in the SOW): downloading, transmitting (for example sending to EPAM e-mail address, external email address or external web-based storage services), copying or otherwise taking (e.g., by screenshots) or retaining any Customer Data (including Confidential Information, Company Information or Protected Health Information) at any time during or after the project execution.
* EPAM employees with Customer accounts must complete any mandatory trainings assigned to them by the Customer. In case of such trainings not yet completed, or If you are not aware of the Customer's policies, immediately ask your Account Manager or Project Manager for a training request.

### 2.3.2     The Internet

So many places to go, so much to see ...but not on EPAM time or equipment!

Did you know that computers record where you go on the Internet? You leave tracks!

Remember these guidelines:

* Use your workstation for authorized business and only for limited personal use.
* Be careful navigating to sites of unknown security.
* Network traffic can be intercepted.
* Do not visit pornographic sites.
* Do not download videos, music or other software that uses large amounts of network resources.
* Do not download or make unauthorized copies of copyrighted materials - it is illegal.
* Several ‘free’ programs come bundled with monitoring spyware.
* Do not install ‘tor’ (Onion Routing). This is forbidden by EPAM policy EPM-SPI\_SoftwarePackageControlWIGLO. Note that it may also be prohibited by law in your country.

**Network Traffic Can Be Intercepted**

On the Internet, information is sent in packets. Hackers can use "packet sniffer" tools to monitor these packets as they watch for words like "password" or "credit card number". Hackers can collect this information, and you may never know it happened.

**Be Careful Navigating to Sites of Unknown Security**

Some Web sites may contain viruses or other malicious code that could damage your computer files. Your computer can become infected and spread it throughout the network. You could be tricked into giving information that could put you at risk. For more information, see Module 5: Internet Safety.

**You Leave Traces of Where You’ve Been**

These traces are called "cookies". They are data files, stored on your hard drive that contain information about your activities on the Web. A website will place them on your computer when you visit it. They store information that might be useful in serving your needs the next time you visit the site.

**Browser Usage**

If you are logged in to an EPAM internal site, do not open any other site by using the same browser, which could be encouraged in a received email.

Although SOP (Same Origin Policy) prevents a site from interfering with the cookies of any other site, it does not prevent an attacker from setting up a website which upon opening performs a malicious act under your authentication credentials - which will ultimately be accumulating on the very same site in which you are currently logged in - and will perform some undesired action(s) without your consent or knowledge.

While it is not easy to create a working CSRF (Cross Site Request Forgery) link and the attacker must have an inner knowledge of the application, still it is not impossible to carry out such attacks, which would work by either clicking on an image or simply by opening a site where the IFRAME sources would carry out the attack without your knowledge.

While CSRF attacks are not easy to perform, they are not impossible. Therefore, you have to be aware of the existence of such attacks.

**Remember to review the Internet Safety Section (Section 5)!**

### 2.3.3     Email

Please, review the Work Instruction: Access to E-mail Services in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_AccesstoE-mailServicesWIGLO.docx).

**Examples of Improper Email Use**

Adrian sends a chain letter email to 10 people...who send it to 10 other people...who send it to 10 other people...by the 8th iteration, more than one billion messages may be sent.

Bob's email to several senior officials contains an unencrypted attachment of a confidential report. The report deals with an ongoing Institute investigation. The report was intercepted and now the investigation has been compromised.

**Ask Yourself These Questions before Sending an Email**

* Should I encrypt the message? Yes, if the message (or attachment) contains sensitive data. Contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)) and they will walk you through the steps you need to take to set up encryption
* Is a digital signature appropriate? Yes, if it's important that the recipient verify that you are in fact the sender
* Is the language and content appropriate? Plain email is neither confidential nor private. Supervisors, LAN administrators, and anyone who might receive a forwarded copy can see your message, so you might want to reconsider the language you use. There should be no sexually explicit, racist, or other offensive language in the message.
* Should I send this email? Certain information should not be sent via email. For example, unencrypted Customer information should never be sent by email.
* Should this message be sent from an EPAM E-mail account? When you send or forward messages from an EPAM email account, those messages are identified with EPAM. This action lends your name and the EPAM reputation to the message, and can make a false message appear authentic. Sending EPAM email is the same as using EPAM stationery.

Please, review the Work Instruction: Data Encryption and Digital Signing in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_DataEncryptionandDigitalSigningWIGLO.docx).

**Email Etiquette**

**Remember**: Do not respond to an entire group list if you only need to respond to one individual.

* Only give your email address to people you know
* Think before responding or forwarding.
* Respond promptly.
* Be clear and organized.
* Use meaningful text in the subject line.
* Only copy people who need to be informed.
* Respect people's time.
* Don't send mail bombs, forward or reply to junk email or hoax message

**Suspicious Emails and Attachments**

You're thinking about opening an email attachment, but something has made you hesitate. Could it be infected?

Be wary of emails if:

* The subject line is strange or unusual.
* You do not recognize the sender.
* It is not work-related.
* If there is an extension or a link which would point to a site.
* You were not expecting the attachment.

**Always encrypt any emails you send with sensitive data!**

**Inappropriate Email**

Never send or forward spam or chain letters! They can cause network congestion and interfere with routing legitimate emails.

* Spam: Mass mailing of information in the form of unwanted E-mail, generally of a bulk or commercial nature. Listserv mailing lists are a popular method of disseminating spam.
* Chain letters: Messages that tell recipients to forward multiple copies which leads to an exponential increase in circulation of the message. Chain letters are recognizable. Some are illegal. And some contain a hoax.

#### 2.3.3.1   Recognizable Parts of Suspicious Emails

A typical email consists of three recognizable parts:

* A hook (catches your interest, e.g., "Make Money Fast")
* A threat (warns of negative consequences if you break the chain)
* A request (asks you to forward the message to multiple addresses)

Letters generally lack the name and contact information of the original sender, making it difficult to verify authenticity.

#### 2.3.3.2   Illegal

Chain letters that ask for money or anything of value are illegal and should be reported to the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).

#### 2.3.3.3   Hoax

EPAM is extremely vigilant about communicating alert information through legitimate security Listservs. Find out if the message is a known hoax.

**What to Do with Unwanted Emails**

Please DO NOT DELETE it!   
Although your first instinct might be to delete or ignore suspicious emails, we ask you to report them by clicking “Report Phishing” button in your Outlook. If you've been targeted by a spear phisher, chances are your coworkers have been too, so by reporting suspicious emails, you can keep EPAM safer.

Once you have reported the suspicious email, you will be immediately notified that your report has been submitted.



Our incident responders will investigate the email as a potential phishing attack. There is no penalty for reporting a harmless email. But if the email is malicious, the intel you have provided will help us determine the attack's source and prevent similar attacks in the future.

You may periodically receive simulated phishing emails that imitate real attacks. These emails are designed to give you a realistic experience in a safe and controlled environment and allows you to become familiar with tactics used in real phishing attacks.

Remember to review the Emails and Email Attachments (Section 5.6)!

## 2.4          Personal Use

Personal use is allowed at the discretion of your supervisor.

Although Chuck knew that IT resources were for authorized business purposes only, he wondered if he could 'legally' use his computer for some personal reasons. The personal use policy allows only limited use. According to this, personal use is allowed if it:

* Is incidental and with minimal cost to EPAM and does not interfere with staff productivity, the EPAM mission, or operations.
* Is not used to misrepresent oneself or EPAM and has no potential for public embarrassment to EPAM.
* Does not compromise EPAM IT systems or security safeguards.
* Does not violate state laws or EPAM policies.

**Information Management**

**3.1          Agenda**

The current tutorial will introduce you to the rules of Confidential Information Management.

**3.2          Objectives**

The objectives of this section are as follows:

* Recognize different types of confidential information that must be protected at EPAM (proprietary information, confidential financial records, etc).
* Learn how to safely manage confidential information (electronic and paper) in different environments.

**3.3          Security Planning**

Computer security efforts are based on:

* The sensitivity of data - the need to protect it from unauthorized disclosure, fraud, waste or abuse.
* The operational criticality - the impact on the programmatic mission of the system if the system is interrupted due to downtime, fraud or abuse.

**3.4          Classification**

Do you work with any systems that are considered to be highly confidential or highly critical?

**Classification** is based on the type of data and the requirements of certain laws.

EPAM Systems has established a general classification framework based on data sensitivity. The classification framework defines the appropriate security levels and protection controls when accessing sensitive information during handling, storing, accessing, transmission, speaking, watching on monitors / computer screens, archiving, destroying and securing physically. See more details in *Guideline: Information Asset Management* in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/doc_GDL_InformationAssetManagementGuideline_B76D4684.html?nodeId=57837e27).

Information assets are grouped by the following categories:

* Project Data – the information is created during the project life cycle. It can be Project Sensitive, Project Confidential; Program Confidential, or Customer Confidential.
* Personal Data – personal information of an individual (See more details and examples later). It can be *Personal Sensitive*, *Personal Confidential*, or *Personal Public*.
* Company Data – information owned by EPAM Systems. It can be *Company Sensitive* or *Company Confidential*.
* Public Data – the information is in the public domain and freely available to anyone and everyone, and any other information asset that has been appropriately investigated and approved to be used as *Public Data*. Only EPAM Management Team is authorized to reclassify *Company data* or Project *data* as *Public* by publishing such information for the public or by making an organization-wide announcement about the reclassification.

**3.5          Protecting Information Assets**

All users are required to read the EPAM Work Instructions at [PAL](https://pal.epam.com).

**Safeguard Scenario**

Angel's job is to enter patient information into a medical database.

Review the following safeguards she uses:

* A privacy screen on her monitor keeps others from viewing confidential data.
* She uses a strong password, keeps it a secret, and changes it often. Angel also has a password-protected screen saver that activates after 10 minutes.
* When leaving her office, she locks or logs off her computer.

**Managing Email**

Rita stared in disbelief at an email that had been forwarded several times. Although it concerned a highly confidential agency matter, some of the emails contained inappropriate comments. Realizing the potential consequences, she sent a message to each of the senders about:

* Confidentiality  
  Did any of you think about security here?  
  Email is NOT secure or confidential and you cannot control who reads it. Think about that the next time you make an inappropriate comment in an email.  
  With Outlook, you can use the options to label an email as confidential. The recipient will see this label in the header of the message: "Please treat this as Confidential".
* Encryption  
  For highly confidential information, you may want to consider encryption. In addition, digital signatures can be used to confirm the identity of the sender. Contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)) to learn how to use these technologies.
* Recipient verification  
  Based on the sensitivity of this email, names and addresses may need verification. There are a lot of people with the same name.
* Authenticity issues  
  Any email address can be spoofed.  
  You might receive an email from your superior asking you to send the reply to *another* email address. The email was spoofed by a hacker.  
  Immediately contact the person who was impersonated by the hacker.

**USB Flash Drives**

Whether it's a smart phone, tablet, PDA, digital camera, or flash drive, the same basic principles governing the protection of data on the desktop apply to all forms of portable media and the systems they reside on.

Current computer models have one or more USB ports for attaching various devices, e.g., digital cameras, portable hard drives, and flash drives/pen drives.

Practice precautionary measures to help protect your data and be cautious of these security threats:

* Introduction of malicious software:  
  Flash drives are excellent vessels for transmitting viruses and worms and can be used to upload spyware that capture passwords or other confidential information.
* Theft or loss of data:  
  It is easy for someone to steal data in large quantities very quickly. If you leave your flash drive on your desk or lose it on the street, anyone who finds the device will have your data.
* Precautionary measures to help you protect your data:
  + Physical security is the key - be careful where you store these drives.
  + Use built-in security features of devices such as password protection, biometric fingerprint reader, or encryption capabilities.
  + Lock your computer and use a password-protected screen-saver with a short idle time.
  + Consider additional, highest-complexity password and encrypting options for confidential files on your computer.
  + Scan files before opening them to protect against viruses.
  + Keep your antivirus software up-to-date.

**Printing Information**

Courtney is the office manager for a team of scientists. Making the rounds through the laboratory, she occasionally finds confidential documents left at printers, copying machines, and fax machines. At the staff meeting she reminds them to take precautions:

* Verify printer locations before sending and pick up documents immediately.
* Label confidential documents and keep them in a secure location.
* Shred or dispose of confidential documents in appropriate trash receptacles when no longer needed.

**Portable Devices**

Laptops and other portable devices must be operated securely. EPAM IT Security policies and procedures apply to these devices also and should be enforced in accordance with the capabilities of each device.

* Laptops and other devices accessing EPAM data should have password protection.
* BitLocker must be installed. EPAM automatically applies BitLocker for full disk encryption in all EPAM laptops. If you have any problems, request Support team to help ( <https://epa.ms/request-encryption>)..
* Store confidential information in accordance with EPAM Policies.
* Encrypt sensitive data communication.
* Devices should timeout/lock after 10 minutes of inactivity.
* Report lost or stolen portable devices and removable media to EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).
* Prior to disposal, surplus or transfer, erase all data on the device. Erase portable devices using local or remote commands (configure them for remote erasure if it is supported).
* Documents containing confidential or internal EPAM information (including personal data) shall not be image captured using a camera (digital or analog), including cameras found in portable devices (i.e. cell phone, smart phone, tablet, PDA, notebook, Webcam, etc.)..

**3.6          Data Privacy**

Data privacy laws regulate the use, handling and cross-border transfer of personal information.

* Personal information “Personally Identifiable information”, “PII” or “P2” means data which relate to a living individual who can be identified:
  1. from those data, or
  2. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
  3. includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
* A subset of PII is “Sensitive”, which by law requires even higher security standards. Sensitive Personal Data are personal data, revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
* “Handling” covers all forms of collecting, storing, transmitting, and using personal data. Personal Data shall be handled confidentially.

**Examples of Personal Information**

* Name;
* E-mail address;
* Personal address;
* Location information;
* Performance appraisal;
* Date of birth;
* Marital status;
* Any other type of Personal data, which is not Sensitive Personal data (see section below)

**Examples of Sensitive Personal Information**

* Race or ethnic origin;
* Political opinions;
* Religious or philosophical beliefs;
* Trade union membership;
* Biometric data;
* Genetic data;
* Sexual activity or sexual orientation;
* Health (medical information);
* Administrative or criminal proceedings and sanctions;
* Financial data;
* Payment/financial instrument details;
* Credentials;
* Personality profiles;
* Combination of name and specific types of Personal data;
* Governmental ID;
* Social security measures;
* Mobile phone number (applicable for China only)

**About photographs**

Photographs, by their nature, may contain sensitive personal information by revealing persons' racial or ethnic origin, while there are captured situations which merely increase the likelihood of associations. A picture showing someone sitting in a wheel chair, even in the garden of a hospital, could be treated as sensitive, since it might reveal health status. Sensitivity of such information is obvious if the photo is accompanied with other personal data such as name etc.

To prevent misinterpretation / security breach, EPAM projects that access personal data shall handle photographs confidentially, like "Sensitive Personal Information".

**How to deal with Personal information**

Personal Information should be:

* Processed fairly and lawfully
* Used only for the specific purposes for which it was collected
* Relevant and not excessive
* Kept accurate and up-to-date
* Retained for a limited time
* Kept secure
* Transferred responsibly to third parties; not transferred across borders without proper measures
* With respect for the rights of the individual data subjects

**3.7          Sharing Files**

Options for file storage and file sharing are defined by the signed contract per projects. However, there are general restrictions for data types not controlled by those contracts.

**Restrictions about data types**

Commercially sensitive Customer data and Customer personal data is localized to the Customer IT environment, EPAM has only remote read-only access, and the transfer and/or the ability to copy such data to EPAM’s IT environment should be technically prohibited by Customer. Storage and/or transmission of Confidential / Sensitive data, i.e., Personally Identifiable Data (PII), Sensitive Personal Information (SPII), Personal Health Information (PHI), Payment Card Information (PCI) and restricted intellectual property shall be under Customer control – EPAM must not have admin rights over these areas.

In other words, EPAM only accepts remote, non-capturable access to the production data. Non-capturable means even creating screenshots of the personal information shall be technically prohibited.

**Where not to store**

 In general, *EPAM shall not store or host Customers’ production data* regardless of the storage media is

* A dedicated or shared EPAM server;
* The EPAM cloud;
* A virtual server based on a contract between EPAM and a third party cloud service provider (instead, the Customer shall sign a contract with the cloud operator, not EPAM);
* Public web storage such as Dropbox, etc. is strictly forbidden. If you upload documents, files, screenshots, text clips etc. to a public service on the Internet, you cannot control them anymore, since they might be collected or shared with others. Do not download Customer files from such public services - instead, inform the Project manager immediately.
* An email with attachment stored in EPAM Outlook;
* A local hard disk in any EPAM workstation/laptop,
* A file in a mobile phone;
* etc.

**Where to store - Internal resources**

Always use the contracted storage options if defined. For *non-PII* and *non-sensitive* data, *unless there are contractual restrictions*, you can use internal EPAM resources for storing company- and Customer-related information such as:

* Confluence/KB is the main platform to store, edit and collaborate on wiki-like and HTML content.
* Target example: [https://kb.epam.com/display/<project-code>/](https://kb.epam.com/display/%3cproject-code%3e/)...
* Sharepoint is the main alternative to store and collaborate in editing or sharing office documents with Word, Excel or PowerPoint.
* Target example: [https://sharepoint.epam.com/Project/<project-code>/](https://sharepoint.epam.com/Project/%3cproject-code%3e/)
* Project file storage for various type of files (binaries, etc).
* Target folder: [\\epam.com\Projects\<your\_location>\<your\_project\_code>\](file:///\\epam.com\Projects\%3cyour_location%3e\%3cyour_project_code%3e\)
* EPAM Video Portal for video files storage.

**Where to store - External resources**

EPAM also provides external resources to store project-related information *unless there are contractual restrictions*. However, it is forbidden to use the below solutions for storing any Personally Identifiable Information (i.e., PII/PHI/PCI) or Sensitive Intellectual Property. EPAM has:

* An enterprise subscription for Office 365 products;
* OneDrive for Business is available for document sharing and collaboration;
* Office Online applications (Word, Excel, PowerPoint, OneNote);
* Information Rights Management solution based on Microsoft Azure RMS.

**3.8          EPAM Security Policies and Procedures**

EPAM security policies and procedures were developed to ensure that adequate and proportionate security controls are set within the organization to safeguard information and intellectual property assets. Policies and procedures are available at [PAL](https://pal.epam.com/).

* Every employee must comply with EPAM’s Code of Conduct and with the Information Security Policies and related procedures.
* Project members must comply with Customer data privacy requirements as well.
* Disclosing EPAM or Customer data in any form is forbidden.
* Disclosing confidential information is a serious security breach.
* Make sure you have completed and behave in compliance with the following trainings:
  + EPAM Annual Information Security Awareness Training (this training)
  + EPAM Data Privacy Awareness Training

**4. Local and Remote Access**

**4.1          Agenda**

The current tutorial will introduce you to the rules of local and remote access.

**4.2          Objectives**

The objectives of this section are as follows:

* Learn how EPAM controls local and remote access.
* Recognize the risks and responsibilities associated with user access.
* Understand the importance of password protection and how to create strong passwords.
* Review remote access requirements.

**4.3          What Are Access Controls?**

Review the *Work Instruction: Access to Systems and Applications* in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_AccesstoSystemsandApplicationsWIGLO.docx).

* Access controls keep out unauthorized users and limit what authorized users can do.
* Authentication requirements can be built into software to limit what information or resources an authenticated user can access and use.
* Access controls can stop users from reading, copying, stealing, deleting, disclosing or modifying confidential information.
* Controls can also help prevent access that is above and beyond a user’s access privileges.

**4.4          Who Gets Access?**

EPAM deactivates user accounts when staff or contractors become inactive or leave EPAM.

Accounts remain active only if a person continues EPAM work.

**IDENTIFY authorized users by:**

* User ID: *New system users are assigned an account with a User ID. Authorization and access rights are assigned to this account.*
* MAC Address: *The MAC address is a hexadecimal number that uniquely identifies every computer of any manufacturer. Do not confuse it with the IP address that can vary for any computer based on the network (segment) it is connected to.*

**AUTHENTICATE valid users with:**

* Password
* Biometrics: *In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes*
* Digital signatures: *A digital signature is a code that is attached to an electronically transmitted message that will uniquely identify the sender. The purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are used in electronic commerce and anytime a higher level of authentication is desired.*
* Other forms of cryptography

**4.5          Risk**

**Uncontrolled Access = High Risk**

Unauthorized users may try to obtain confidential EPAM information for personal gain, or malicious purposes (to discredit EPAM, to launch attacks on critical infrastructure, etc.).

Authorized users with malicious intent are a high risk because they are "trusted" users, they know the system and have access to it, and therefore are capable of doing a lot of damage before detection.

What happens if someone enters my User ID and knows my password?

**4.6          Understand Access Responsibility**

As a kind of legal prevention, a warning message appears when you log on to your computer, stating:

*“This system is owned by EPAM Systems. If you are not authorized to access this system exit immediately. Unauthorized access to this system is forbidden by company policies, national, and international laws. Unauthorized users are subject to criminal and civil penalties as well as company initiated disciplinary proceedings. By entry into this system you acknowledge that you are authorized access and the level of privilege you subsequently execute on this system. Your further acknowledge that by entry in this system you expect no privacy from monitoring.”*

**4.7          Password Requirements**

All EPAM IT users must create strong passwords.

The ‘Password’ section of the *Work Instruction: Access to Systems and Applications* in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_AccesstoSystemsandApplicationsWIGLO.docx) includes useful resources for selecting good passwords.

* Use mixed-cased letters, numbers, punctuation, and special characters.
* Keep it easy to remember and hard to guess. Example: Re4$!freR.
* Make it at least 9 characters long and change it at least every 3 months.
* Do not use easily guessable passwords, such as your or family members' name, phone number or date of birth.
* Do not use proper names or dictionary words (in any language).
* Do not use the same password for all systems you access.
* Memorize it and keep it a secret; do not share it with anyone.

A weak password puts EPAM data and the whole network at risk!

The following tips can be useful for selecting a good password:

* Take two familiar things, wrap them around numbers and special characters (dogs8#cars).
* Use the initial letters of a phrase, especially if a number or special character is included. E.g. "One for the money, two for the show" becomes O4t$,24ts
* There are web tools to learn how strong a password is. Example site: <https://blog.kaspersky.com/password-check/> **Warning!** Never enter your actual or planned password in such sites!!!

**4.8          Password Self-Service Management**

When the password is changed, it is important to update stored credentials in the most frequent account lockouts sources:

* Stored user names and passwords in Windows Credential manager
* Third-party software password managers (like Mozilla Firefox, Opera, Google Chrome)
* Wi-Fi stored passwords
* Mobile mail clients
* Source Control clients (GIT)
* SQL Reporting services (Execution Account)
* Windows services and scheduled tasks
* Disconnected Terminal Server sessions
* Persistent drive mappings

**Otherwise, your account may be sporadically locked out due to multiple failed logon attempts**. Often user accounts are locked out through corporate applications such as PMC, Exchange CAS servers, Wi-Fi authentication servers.

Find more info at: [Password self service management](https://support.epam.com/esp/ess.do?ctx=docEngine&file=kmdocument&query=id%3D%22KM0077%22&action=&title=Knowledge%20Document%20KM0077)

Registration is mandatory; please visit [password.epam.com](https://password.epam.com) and complete the registration as soon as possible.

**4.9          Access Responsibilities**

If others need access to your information, make the necessary arrangements to avoid sharing your password.

* Only access those systems that are necessary to perform your job.
* Levels of access (e.g., read, modify, delete) should match assigned duties.
* Access rights are for official duties.
* Do not share or intentionally compromise your password.
* If you realize that someone knows your password, change it immediately and report the incident as soon as possible.

**4.10       What Is Remote Access?**

Please review the Work Instruction: Remote and Guest Access to Corporate Network Resources in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_RemoteandGuestAccessToCorporateNetworkResourcesWIGLO.docx).

EPAM offers approved users the ability to access the EPAM network from external sites. Remote access may be set up on:

* An EPAM-supplied computer, or
* A personal computer used for EPAM work.

**Note:** Use of a personal computer puts even more responsibility on the user to maintain security standards.

Do not access EPAM resources from publicly available computers (Internet cafe) - many of them run spyware/logger programs.

Remote access options are EPAM VPN and TSG (Terminal Service Gateway).

This is managed centrally by Global IT. Requests for alternative remote access methods must be submitted to the IT Security Department.

**4.11      Remote Access to EPAM Network**

All EPAM remote users are required to review the *Work Instruction: Remote and Guest Access to Corporate Network Resources* in [PAL](https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_RemoteandGuestAccessToCorporateNetworkResourcesWIGLO.docx).

As an authorized remote access user, take the necessary steps to:

* Keep your Remote Access password private, even from family members.
* Keep your **antivirus software** up to date on your remote computer(s).
* Check your computers for required **software updates and patches**.
* Run a personal **firewall** on any home systems used for remote access.
* Scan for **spyware** on your remote system.
* Delete all prohibited software from your personal workstation (torrents,p2p clients, etc.)
* Avoid interacting with **suspicious or unsolicited emails** and immediately delete them.
* Avoid clicking on links in **Pop-up Ads**.

If you are not doing **all** of the above, then you are not taking full responsibility for securing your remote computers.

* Firewall: *Computer hardware or software that prevents unauthorized access to private data by outside computer users (as through the Internet).*
* Spyware: *Spyware is a general term for a program that surreptitiously monitors your actions and collects and sends information to an outside party, where it is stored in a database for analysis. Spyware could be used to monitor your connection to the EPAM network and gain access to confidential data. Spyware can often be hidden in the guise of a useful program, like a game or a program that allows you to enhance your email. Pop-up ads can also be a source of malware, like spyware, viruses, worms, and Trojan horses.*
* Antivirus software: *Antivirus software is a program designed to identify and remove known or potential computer viruses.*
* Software updates and patches: Please contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)) or support staff and request them to update your computer's operating system to the latest patch.
* Suspicious emails: *Suspicious emails include unnecessary characters in subject lines, only first names in the "From" field, requests for your personal information like bank/credit account numbers, social security numbers, passwords, PINs, etc., notifications that you have won something, requests for assistance from someone you do not know, and .zip file attachments that require you to enter a password.*

**Note:** Similar suspicions should apply to instant messengers, such as Skype

* Pop-up ads: *Certain Web sites contain code that automatically launches a new browser window containing an advertisement. An advertisement launched this way is called a pop-up ad. Frequently, such ads contain links, and sometimes the entire ad is a link. The danger here is in the links. For example, a less reputable organization may have the link lead to download of spyware, or a hacker may insert malicious code that downloads when the link is clicked.*

**4.12       Working with Wireless Devices**

Working with wireless devices is an essential part of computing today.

Threats include:

* Interception by attacker
* Session takeover
* Rogue AccessPoint for stealing authentication
* Insertion by attackers
* War driving
* Denial of service

If you are required to connect a laptop to the EPAM wireless network please contact EPAM Support Team for assistance ([SUPPORT.EPAM.COM](https://support.epam.com/)).

**It is prohibited to connect personal Wireless Access Points to the EPAM network**.

Wireless devices are increasingly becoming a target for hackers.

The term “war driving” describes driving around with a laptop, a smart phone or a PDA in one’s vehicle, detecting Wi-Fi wireless networks.

Hackers can intercept sessions, hijack sessions and even issue a denial of service.

Always use firewall and antivirus when you connect to a wireless network.

**5. Internet Safety**

**5.1          Agenda**

The current tutorial will introduce you to the rules of Internet Safety.

**5.2          Objectives**

The objectives of this section are as follows:

* Identify different types of malicious logic.
* Recognize signs and symptoms of a malicious logic infection.
* Recognize the ways malicious logic can spread.
* Identify prevention and protection strategies.

**5.3          Vulnerability of the Company**

**Why is EPAM vulnerable?**

When connected to the Internet, all computers and networks - including the EPAM network - are susceptible to attacks, unauthorized use or access. One compromised computer can affect every other computer sharing a connection.

EPAM has strong security controls at the EPAM perimeter, network servers, and desktops, and uses a firewall to filter traffic from the Internet.

However, constant vigilance is required to protect and update IT resources with the latest patches and upgrades.

The majority of successful attacks from the Internet can be traced to vulnerabilities that people know about but haven't fixed yet.

True or False? *True - It is the user's responsibility to patch and upgrade systems to ensure safe computing.*

**5.4          Patch**

A piece of software code to temporarily fix an existing problem or vulnerability.

**5.5          Intruders**

**5.5.1     Social Engineering**

Social Engineering is a non-technical kind of intrusion relying heavily on human interaction, which often involves tricking other people into breaking normal security procedures. The attacker uses social skills and human interaction to obtain information about an organization or their computer systems.

Most experts agree that social engineering is generally a hackers manipulation of the natural human tendency to trust. The weakest link in the information security chain is the natural human willingness to accept someone at their word. This is exactly what makes us vulnerable!

A social engineer runs what is typically known as a "con game". A person using social engineering to break into a computer network generally gains the confidence of someone who is authorized access to the network, in order to help reveal information that compromises that network's security.

**Various Methods**:

* The first and most obvious is a simple direct request.
* Dumpster Diving - A term used for going through the trash (or dumpster) to obtain information that can be used to steal one's identity. It is truly amazing the things people discard that can be helpful in finding additional information about a person they are potentially targeting. Dumpster diving is not technically "social engineering", but it can sometimes be deployed as a step towards getting helpful information .
* Raiding Mailboxes - Once the person has selected a victim, raiding that persons mailbox can often lend additional information to be used against them. The more you know about a person, the more effective alternate means of gaining data become.
* Phishing is one of the newer forms of social engineering - It involves creating and using e-mails and Web sites designed to look like those of well-known legitimate businesses, financial institutions, and government agencies to deceive Internet users into disclosing their personal information. Phishing scams typically operate counterfeit web sites that lure consumers into revealing their personal and financial data, including social security numbers, bank and credit card account information, and details of online accounts and passwords.
* Impersonation - This is a method where the attacker pretends to be someone in an authoritative position. Some of the methods used during impersonation attacks include... acting as an IT support or Support Service employee, a repairman, a supervisor or manager, or a trusted third-party vendor.
* Surfing Company Web Sites - A lot of corporate information can be obtained before even talking to anyone by simply surfing company web sites, like employee email addresses and phone numbers, organizational charts, executive titles, financial information and more.

**Where do intruders come from?**

How many countries are developing information warfare capabilities?

More than 100 countries. Cyber terrorists will likely try to spread their views through spam or Web defacements. They could also target a critical infrastructure (e.g. financial, transportation, or communication industries) to cause an economic or other critical impact.

Anywhere, at any time, intruders can attack, often hiding their identity.

**Who are these threat agents?**

* Teenage pranksters
* Hacker junkies
* Disgruntled former employees
* Terrorists or criminals
* Foreign intelligence agents

**5.5.2     Intruders' Toolkit**

**How easy is it to hack?**

An attacker could exploit your system with hacking tools fairly easily if you are directly connected to the network (not using a router) and the attacker knows your IP address.

Fact: According to NIST (National Institute of Standards and Technology), hackers post 30-40 new tools to the Internet hacking sites every month.

**Intruders' toolkit**

* **Vulnerability scanning:** Internet hackers constantly scan networks to try and identify where systems are vulnerable.   
  Pre-Attack Probe is another name for this type of scanning.
* **Password Cracker:** Intruders use a program that automatically keeps trying to log in to a system using a series of easily guessed passwords, or using a dictionary as a source of words.
* **Network Spoofing:** Intruders set up a program that impersonates the sign-on routine for another system. When you attempt to log in to the system, the intruder's program collects your password, and then returns a message that the system is unavailable. These programs can collect hundreds of valid passwords.
* **Viruses:** A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. Copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files.
* **Worms:** A worm is an independent computer program that reproduces by copying itself from one system to another across a network. Often triggered when someone opens an infected email attachment, the worm program can send replicas to everyone listed in the person's mail directory.
* **Logic bombs:** A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as the salary database) should he ever leave the company.

**5.6          Emails and  Email Attachments**

Email attacks, such as email spoofing, phishing, etc., can potentially harm great number of users.

**Think Before You Click**

Consider the following before opening any suspicious email:

* Do you know the sender?
* Have you received email from this sender before?
* Were you expecting a message (particularly one with an attachment) from this sender?
* Does the email header (sender, subject line, attachment names) make sense? Does it contain any strange characters?
* Does the attachment name seem to match with the sender and the subject line? Does it contain poor spelling and grammar?
* Does this email contain a virus? Your Symantec antivirus software will tell you this if it is installed, running, and maintained as described earlier in the course.
* Do not click on links embedded in spam emails even they seem to be secure/correct. That is, they can contain strange characters, e.g., Cyrillic ones.
* Don’t buy things or make charitable donations in response to spam email.

**Think before opening email attachments**

* Malicious email is a common form of social engineering.   
  The attachment may contain a ‘reverse connected shellcode’ in an encoded form therefore the antivirus tools cannot identify them as a threat. However when you click on it, the shellcode ‘reverse-connects’ to the attacker's computer, thereby creating a valid session.   
  Please note that your firewall, even the applied security mechanism which was applied in the network - might let this connection be established!
* Scan all email attachments for viruses before opening them.
* Do not open email attachments from unknown sources.
* Use email filtering software.
* Many of us still fall victim.
* The strongest weapon against this type of attack is recognizing common ploys and always thinking before clicking.

**5.6.1       Suspicious Emails and Attachments**

* If you're thinking about opening an email attachment, but you believe the email to be suspicious, it could be infected. Be wary of emails if...
* The message asks for personal information.
* The subject line is strange or unusual.
* You do not recognize the sender.
* It is not work-related or you didn't initiate the action.
* If there is an extension or a link to an unfamiliar site.
* The message contains poor spelling and grammar or has no EPAM disclaimer/signature.
* You were not expecting the attachment.
* Finally, even when opening emails from trusted sources, you should not open suspicious attachments.
* Please be cautious when going through your emails. We depend on your security awareness!

**5.6.2       Suspicious file extensions**

* Files with extensions .vbs, .exe, .com, .shs, .bat, .cmd, .inf, .sct, .vbe, .vb, .wsc, .wsf, and .wsh are suspicious. However, virtually any extensions should be red flags if you received the email from an unknown sender.
* For example, do not open the filename: "Gotcha.exe". Do NOT!
* The EPAM email system now strips many of the attachments that historically have been associated with viruses. However, you must be careful with home computers.

**5.6.3       Security measures for when you receive a suspicious email**

* In order to protect yourself and sensitive company information, please keep in mind the following security measures when you receive a suspicious email:
* Do not click on any links.
* Do not open attachments or run macros if you have opened an email from an unknown sender.
* Do not respond to suspicious email.
* Do not enter your credentials after clicking links.
* Delete the email to prevent yourself from opening it accidentally.
* Always use your EPAM employee signature and disclaimer when you send emails.
* Use mail encryption as often as possible.
* If you are not sure whether or not you should open an email, ask your manager.
* Notify the EPAM Support Team (SUPPORT.EPAM.COM) about suspicious emails.

**Do not forward suspicious emails.**

If you need further assistance, please contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).

**5.6.4       Spyware**

**Don’t Let Spyware Capture Your Personal Information**

TIP: Toolbar "helpers" that offer to enhance email messages generally contain spyware.

Spyware is a general term for a program that surreptitiously monitors your actions and collects and sends information.

Users are often tricked into downloading and executing spyware by attaching it to an otherwise useful piece of software, such as a game or a program to enhance your email design or store your passwords.

Some spyware programs are sinister, like a remote control program used by a hacker.

Others may be more prying than malicious. For example, software and other companies have also been known to use spyware to gather data about customers - a practice that is generally frowned upon.

Spyware could also be used to monitor your connection to the EPAM network and gain access to our confidential data.

Is spyware watching you? Look for these signs:

**Signs and Symptoms of Spyware on your System**

Spyware can be hard to spot because the symptoms often appear to be normal Web or computer operations, but here are some things to consider:

* **Suspicious and/or Excessive Pop-Up Ads:** Many legitimate Web sites contain pop-up ads, and spyware tries to mimic those ads. So there are no guarantees, but if the content of the ads seem strange, they may be from spyware. And, if you're getting pop-up ads when you're not connected to the Internet, it's very likely they are coming from spyware.
* **Poor System Performance:** If you've noticed a significant drop in responsiveness lately, it could mean that spyware is draining your computing power. Some specific symptoms include:
  + Computer runs slower in general
  + Computer takes longer to start up
  + Computer stops responding randomly
  + Illegal operation errors occur
* **Strange Internet Browser Behavior:** Many forms of spyware target your browser.  
  Common problems include:
  + Browser crashes
  + New favorites: Some spyware add "favorites" of their own to your browser's favorites folder. If you notice an unusual number of new favorites and are not sure how they got there, spyware may be to blame.
  + Your default homepage has changed: One of the oldest spyware tricks is to automatically change your Web browser's default or start-up homepage.

If you need further assistance, please contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).

**5.6.5       Phishing**

One of the newer forms of social engineering, phishing involves creating and using emails and websites designed to look like those of well-known legitimate businesses, financial institutions, and government agencies to deceive Internet users into disclosing their personal information. Phishing scams typically operate counterfeit web sites that lure consumers into revealing their personal and financial data, including social security numbers, bank and credit card account information, and details of online accounts and passwords.

**Don't get caught by the phishing hook**

Criminals may try to manipulate your tendency to trust (this is the so-called social engineering) and break into your system and do harm.

Don’t be a victim!

**A Common Ploy**

* Scammers copy the webpage code from a major site—such as a banking or e-commerce site—and use that code to set up a replica page that appears to be part of the company's site.
* Then they send a fake email with a link to this page, which solicits the user's credit card data or password.
* When the form is submitted, it sends the data to the scammer while leaving the users on the look-alike site so they don't suspect a thing.

**How to Avoid the Internet Scam Known as Phishing**

* If you receive an unexpected e-mail saying your account will be shut down unless you confirm your billing information, do not reply or click any links in the email body.
* You may receive emails even from an  @[epam.com](http://epam.com/) user asking you to update your EPAM account by clicking a link. It’s highly likely that the link in those emails will take you to a malicious website. **Do not click such links.**
* Check the terms and disclaimers of an e-shopping site before using its service.
* Check the trustworthiness of the website (e.g. checking the SSL certificate).
* Before submitting financial information through a website, look for the "lock" icon on the browser's status bar or for the "s" following http (i.e., secure sites use https://). It means your information is secure during transmission.
* Use digital certificates for transactions over the web.
* Log out immediately after finishing your e-shopping activities.
* Retain and review your transaction records.
* If you are uncertain about any information, contact the company through an address or telephone number you know to be genuine.
* If you have unknowingly supplied personal or financial information, contact your bank and Credit Card Company immediately.
* Use different passwords for bank accounts, EPAM accounts and external accounts.
* Do not share your IDs with others.

If you need further assistance, please contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).

**5.6.6       Increasing Email Security**

* In order to identify possible fraud emails, EPAM has implemented a rule on EPAM email server. The mail server adds a prefix [Possible fraud sender] to the subject line of the letters from the addressees @[epam.com](http://epam.com/) if they were sent without authentication (anonymously). Messages created with the authentication will not be affected. If an email is marked as [Possible fraud sender] you should not trust the content. Please, do not click any links, open any attachments or take any other actions with it.
* If your system (development server, some 3rd party software service) sends non-authenticated messages, please, order the Auto Account via [SUPPORT.EPAM.COM](https://support.epam.com/).
* Outlook warns you if external email address appears in the To or Cc field.

**5.7          Computer Under Attack**

**How do you know if your computer is infected or under attack?**

You see... a blue screen, or strange items like graphics, odd messages, or system error messages on your monitor.

You experience… a long delay starting up your computer or it's running really slow. You have corrupted, inaccessible, or missing files. You can't access your hard drive or data disks. Your computer has suddenly run out of memory. You have lost control of your computer. You see a lot of pop-up adds.

On the other hand... you might not experience any symptoms and may be totally unaware that your machine has been compromised.

**What should I do if I think my computer is infected?**

At the office, if you think your computer is infected, immediately contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)). Try to record everything that happened to assist with diagnosis.

If you are using an EPAM computer at home, close all your programs, shut down the system, and bring your computer to the office for evaluation, contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)).

**Keep antivirus software up-to-date**

Office Computer:

* All EPAM staff has access to site-licensed virus protection software. Your local IT staff regularly performs software updates to your system.

Home Computer:

* If you connect to EPAM network through your home computer, you are responsible for keeping the computer’s security configuration up-to-date, e.g. keep antivirus up to date, turn firewall on, keep security patches up to date, turn on automatic updates.
* You can also purchase and install security software for your home computer (e.g. web filtering, anti-Spam, anti-Spyware, personal firewall etc.). Consider updating it daily or each time you log on. Set up your computer to scan your computer hard drive automatically once per week.
* For home usage, you may use various tools to remove viruses (we cannot guarantee that removal will be 100% successful):

<https://www.microsoft.com/en-us/download/details.aspx?id=5201>

<https://www.freedrweb.com/download+cureit+free/?lng=en>

<http://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool>

Note that products of one or more software manufacturer, including virus removal tools, may be prohibited by law in your country.

**5.8          Installing New Operating Systems**

Computers must be configured properly to be secure. Many new operating systems arrive in a default mode with security features turned off. This makes your computer extremely vulnerable to attacks from the Internet.

Check with **IT Security Department** if you believe your computer needs to be scanned for vulnerabilities.

**5.9          Surfing on the Internet**

**5.9.1       Preventing Common Threats**

**Be cautious** - installing screen savers, games, or programs from questionable Internet sources is risky - you don't know what software codes might be hidden within them.

**Be aware** - you can get viruses from Instant Messenger-type services, e.g., links to viral files spreading over Skype chat messages.

* If you receive media links in a message, DO NOT click the link. Most likely, the contact's computer is infected and a virus is sending such messages.
* If you receive a message on Skype that contains a link and you are not sure whether it points to a virus or malicious content, ask the sender whether he or she really sent it, before clicking the link.
* If you accidentally access a restricted site (e.g., with pedophilic, racist, pornographic, terror related, or other content), leave it immediately then delete it from your browsing history.
* If you accidentally click a similar link on your EPAM workstation / laptop - create a request in <https://support.epam.com> to scan your computer.
* If you get a similar message from an EPAM employee - let the Support Service know about this.

Also:

* Validate the website you are accessing.
* Be cautious if you are asked for personal information.
* Use encryption to protect sensitive data transmitted over public networks and the Internet.
* Install antivirus, perform scheduled virus scanning and keep virus signature up-to-date.
* Project data should be stored on a server that is backed up frequently. Follow the rules in your project contract.
* Do not download data from doubtful sources.
* Do not visit untrustworthy sites out of curiosity, or access the URLs provided in those websites.
* Do not use illegal software and programs. See the list of approved software at EPAM at <https://kb.epam.com/display/EPMSAM/Approved+Freeware>

**5.9.2       Restricted Protocols**

**Torrent and Peer-to-Peer Communication**

EPAM is in the business of working closely with our clients in creating, managing, protecting and productizing solutions which impact business and lives. Our Business Analysts, Solution Architects, Developers, Testers and every other EPAMer have access our clients' Intellectual Property. We have a collective responsibility to ensure that we handle this responsibly and per the mandate of our clients.

Having said this, now let’s see why are we concerned about Torrent software or any P2P communication.

The importance of controlling Torrent/P2P is not limited to simply preserving bandwidth or potential copyright violation. P2P networks are fundamentally distributed and designed to easily survive the loss of any endpoints. This trait has made P2P increasingly attractive as a safe carrier for botnets. Instead of relying on command-and-control servers that can be taken down, a peer-to-peer based control structure allows a botnet to survive and provide coordination simply by using the end-points of the botnet themselves. Additionally, P2P software also exposes the endpoints directly to the internet when they were otherwise behind a Firewall and not visible to the outside world.

This emphasizes the risk of allowing P2P traffic to run unchecked in the enterprise as it provides cover for malware to hide in the network and ex-filtrate critical organizational information. It is also an obvious fact that applications used to spread malware are the most common or most visible applications and are generally overlooked, which has allowed P2P software to maintain a steady existence, hiding in the shadows of social media and digital lockers.

Therefore, any Torrent/P2P software on EPAM endpoints are **strictly forbidden.**

**5.10       ZERO TOLERANCE**

It is strictly forbidden to operate, use, store, or transmit any of the following, using EPAM resources, including using own personal workstations, laptops during connection to EPAM infrastructure by Wi-Fi, VPN or other channels:

* peer-to-peer software (P2P) including torrent clients/files except authorized software,
* software created for distribution of copyrighted objects (music, movies, etc) without the consent of the copyright holders,
* pornography software, including watching pornography sites,
* key generator and cracking software (including Wi-Fi access cracking applications),
* anonymizers and software that circumvent monitoring/tracking network systems,
* unsupported vulnerable software added to the block list by IT Security team (full list: <https://kb.epam.com/display/EPMSAM/Rejected+Freeware>),
* non-enterprise/non-corporate standard encryption tools,
* cryptocurrency mining software, including usage of corporate resources (hardware, network, etc) for personal profit

If any of the above are discovered, management will consider the situation as a serious breach of internal regulations and the responsible User will be subject to disciplinary action up to and including termination of the User’s contract and/or legal action.

**6. Physical Security**

**6.1          Agenda**

The current tutorial will introduce you to the rules of Physical Security controls at EPAM.

**6.2          Objectives**

The objectives of this section are as follows:

* Recognize physical threats and understand how they make our IT assets vulnerable.
* Learn about the safeguards you can use both inside and outside the office.

**6.3          Physical Security and Protecting Confidential Information**

**Physical security**

Physical safeguards are powerful tools to protect EPAM information assets.

Example situation: Imagine that you return from lunch one day and find that your email screen is up - which is  not the way you left your computer. Your mind becomes a swirl of anxious questions, perhaps panic.

* Who was in my office and why?
* Did they read my email - or send email?
* Did they go through my electronic files, my paper files or my trash can?
* Did the intruder access anything that is confidential?
* What applications did I have open on my desktop?

Failure to adopt secure behaviors leaves your data, and all computers connected to the network, vulnerable! It also places laptops, smart phones, cell phones and ID badges at risk for theft.

**6.4          Securing Your Environment**

**Safeguard Measures**

Access control to perimeter

* Always use your personal entry card.
* Wear your EPAM badge visibly at all times.
* Visitors must be authorized and must sign the log book.
* Visitors must wear their badge visibly and be escorted by a project member at all times.
* If you find a stranger alone in the office or a stranger requests entrance, accompany him/her to the Reception/Security Guard.
* Only authorized support staff under contractual obligation are allowed in the perimeter: electricians, AC maintenance, housekeeping, etc.
* Report lost access cards immediately to Project Manager (PM) and Support Team (SUPPORT.EPAM.COM); afterwards, lost cards must be disabled.
* Report any unauthorized attempts and alerts to PM and Support Team (SUPPORT.EPAM.COM); they must be investigated immediately.
* Do not prop open the entrance door.
* Beware of tailgaters.
* When you leave the office, ensure that the windows are closed.
* Photography is prohibited.

**Working area**

If you work in an area dedicated to a single Customer project, unauthorized persons must not enter the perimeter.  
Always be compliant with the “Clean Desk and Clear Screen” policy. See the document in PAL.

Examples:

* Locking doors/drawers: Use door and drawer locks. Any paper document or portable storage device that is not locked up is vulnerable. Door and drawer locks generally work when you use them.
* Securing trash: Shred confidential materials when discarding. Could "Dumpster Divers" (people who sift through your trash) find confidential information? Remember to shred confidential documents or place them in secure recycling bins.
* Equipment security: Use a secure cable lock, e.g. Kensington lock when your equipment is unattended, even in the office and even for a short period. Property passes are required if taking a PC home.
* Working at home: Secure confidential materials. When working from home, remember to take the same precautions as you would at the office. Remember to think about who could get access to your PC files, including family members.

**6.5          Hazards**

What do hurricanes, fires, floods, ice storms, water leaks, electrical surges, system failures, and hard disk crashes have in common?

They are often unpredictable and can cause a lot of damage to your computer and files if you have not taken any precautions.

**To prepare for the unexpected hazards:**

* Save new documents immediately.
* Set your PC to save automatically every 5-10 minutes.
* Save important files to a server that is backed daily.

**6.6          Theft and Loss**

Waiting for the train, Dr. Green was focused on his smart phone, catching up on email. Oblivious he was being targeted, he did not notice someone picking up his laptop case. Now someone else has the science behind his patent application.

Why are portable devices like laptops, smart phones, tablets etc., so vulnerable?

* These devices are used outside the security of your office environment.
* Small devices can be easily stolen and concealed.
* People often have both personal and office information on these devices.
* These devices are targets for theft because of their street value and the value of information they may contain.

**6.7          Anti-Theft Tips for Portable Devices**

**Protection**

* Be accountable for your IT assets and data.
* Report them if lost or stolen.
* Disguise them from potential thieves.
* Adhere to the EPAM Code of Conduct.
* Use good judgement to protect your data.
* Protect your laptop during trips.
* Ensure sensitive information on the screen is not visible to others.
* Protect your user ID and password.
* Do not store sensitive information in portable device without strong encryption.
* Do not leave your device/sensitive documents unlocked.

**Equipment value**

Protect them as if they were cash. Be aware of your surroundings and never leave devices unattended.

**Hand-held devices**

Immediately report stolen or lost PDAs, cell phones, and other IT equipment to your local IT staff. In addition, report stolen equipment to the Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)) and Project Manager.

**Disguising equipment**

When traveling, divert potential thieves by carrying portable devices (like laptops) in a sports bag rather than a computer case.

**Laptops**

When in the office, laptops should be secured to an immovable object with a computer security cable. Outside the office, never leave your laptop unattended. Strengthen your laptop's security by using fingerprint authentication if that feature is available. Store sensitive information in accordance with EPAM Work Instructions.

Do not leave your laptop unattended in an open freely accessible area even if the laptop is locked with a ‘Kensington lock’.

**Passwords**

Password-protect your devices and enable security features.

**7. Computer Security Review**

**7.1          Agenda**

The current tutorial will introduce you to the rules of Computer Security Review.

**7.2          Objectives**

The objectives of this section are as follows:

* Review your current computer security habits in light of threats and vulnerabilities.
* Review safeguards that can be easily adopted to help ensure the security of your desktop computer.

**7.3          Help References**

**Can you answer these questions?**

* Where are computer security policies and guidance located?

*Work Instructions and guidance are accessed from EPAM Process Assets Library (PAL):* [*https://pal.epam.com*](https://pal.epam.com) *Remember: the IT Security Department can help you interpret the policies.*

* Who is available to assist with computer security problems?

*Your major sources for help are:****EPAM ITSD (IT Security Department):*** *IT Security specialists to assist you with security policies, issues, and problems. (*[*WFT IT Services Security*](mailto:WFT%20IT%20Services%20Security%20%3CWFTITServicesSecurity@epam.com%3E)*)***EPAM Support Team**: For technical and security problems, theft of equipment, and for reporting incidents of suspected computer fraud, waste, or misuse. ([SUPPORT.EPAM.COM](https://support.epam.com/))

**7.4          Office Workstation**

**How vulnerable is your office workstation?**

* Can people walk up and access it?
* Should I have a privacy screen so that no one else can see what is on the monitor?
* Do I have a password-protected screen saver?
* Do I have a lock workstation feature on it?
* Do I log off and shut down when leaving for the day?
* Do I regularly back up important files, or save them to the network server so I will always have copies in case my computer files became corrupted?

**Password-protected screen saver**

These are screen savers that automatically start after a predefined period of computer inactivity. Once the screen saver is activated, password reentry is required to access the computer.

**Lock workstation**

Windows operating systems allow you to lock your workstation. By simultaneously pressing on the Ctrl, Alt, and Delete keys, and then clicking on Lock Computer, or pressing Win+L the computer gets "locked" and requires a password for reentry.

**Log off and shut down**

Logging off and shutting down helps reduce the threat of someone else accessing your computer.

**Are your passwords well selected?**

* A mix of at least 9 characters using letters, numbers, punctuation, and special characters (e.g., 2ro$Bots!)?
* Easily remembered but difficult to guess?
* Never posted, shared, or stored in your workstation?
* Changed at least every 3 months?

**Antivirus protection**

What if you knew you could get viruses, worms, or other malicious software infections from the Internet, e-mail attachments, infected disks, new shrink-wrapped software packages, Palm Pilots, chat rooms, and instant messaging services?

You would be more careful, RIGHT?

* Keep antivirus software up-to-date in the office, at home, and on all portable devices (e.g., laptops).
* Be careful downloading any type of programs from untrusted Internet sources.
* Don't open suspicious email or instant messenger attachments.
* If an antivirus system warning pops up warning you that the program has been disabled, or you see a small icon on the system tray saying that the antivirus/firewall system has been deactivated and despite the fact that you have just turned it back on, it deactivates again, unplug the computer from the network immediately and contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)) promptly.

At the office, if you think your computer is infected, immediately contact the EPAM Support Team ([SUPPORT.EPAM.COM](https://support.epam.com/)). Try to record everything that happened to assist with diagnosis.

If using an EPAM computer at home, close all your programs, turn off the machine, and bring it into the office for evaluation.

**Full disk encryption**

BitLocker must be installed. EPAM automatically applies BitLocker for full disk encryption in all EPAM laptops.

* If you have any problems, request Support team to help ( <https://epa.ms/request-encryption>).
* Expecting your cooperation by opting for encryption at the earliest.

Encrypt files containing personal information if they

* Are classified as a Sensitive data
* Travel across public networks
* Are transmitted either over wire or wirelessly
* Are stored on portable devices

Unless the Customer requests another method, X509v3 private certificate should be used to encrypt files, folders, emails.  
Please see more about encryption in Work Instruction: Data Encryption and Digital Signing in PAL.

**Why use encryption?**

Disk encryption ensures that files are always stored on disk in an encrypted form. The files only become available to the operating system and applications in readable form while the system is running and unlocked by a trusted user. An unauthorized person looking at the disk contents directly, will find garbled random-looking data instead of the actual files.   
Disk encryption can prevent unauthorized viewing of data when the computer or hard-disk is:

* Located in a place to which non-trusted people might gain access while you are away
* Lost or stolen, as is often the case with laptops, netbooks or external storage devices
* In the repair shop

In addition, disk encryption can also be used to add some security against unauthorized attempts to tamper with your operating system – for example, the installation of keyloggers or Trojan horses by attackers who can gain physical access to the system while you are away.

Warning: Disk encryption does not protect your data from all threats.

Warning: Your data is not protected if you share the encryption key with others, if you keep the key in a public place, or if you apply an easy-to-guess key.

Warning: Disk encryption also will not protect you against someone simply wiping your disk. Regular backups are recommended to keep your data safe.

**7.5          Backup**

Regular backups are recommended to keep your data safe. Follow the rules in your project contract.

Save files frequently: Set computer(s) to automatically save every 5 - 10 minutes.

Important files should be saved and stored in internal locations offered by EPAM, i.e., Personal or Projects file storage.

**7.6          Remote Access**

If you use remote access to connect to the EPAM network, you should review the policy that explains how you use it.

Did you know?

* Security rules for office workstations also apply for remote access.
* Antivirus protection must be up-to-date.
* Passwords should never be stored in a login script. If you are logging onto a system and a window pops up asking if you want to save your password - don't do it. This could make it very easy for someone else to access your system.
* Remote access to any desktops/laptops within the Customer’s project perimeter depends on the agreement with the Customer.
* Remote access (e.g., from an EPAM user’s home) is not allowed unless special written approval is obtained from/through the PM (other routes shall be technically blocked).
* Transferring Customer data to removable media is forbidden.

**7.7          Email: Things to Remember**

* Email is not secure - encrypt sensitive information.
* Forwarding chain letters is illegal - delete them.
* Attachments may contain viruses - be careful.
* Email is like official EPAM stationery - think before you send anything.
* Don't respond to a group list - unless you really want to send your message to everyone.

**7.8          The Internet: Things to Remember**

Be careful about the types of information you divulge over the Internet!

* You don't have to be a high profile user to be targeted by a hacker.
* Computer systems must be secured with all required security patches (fixes) before connecting to the Internet to avoid being hacked. Periodically, additional patches may need to be installed to protect against new vulnerabilities. It is your responsibility to make sure this happens.
* Websites and programs downloaded from the Internet may contain viruses or other malicious software that could infect your workstation. Be careful what you download.

**7.9          Never Consider**

**Never consider**

* Downloading or using unauthorized copies of copyrighted material or software.
* Installing or running security programs that reveal weaknesses in EPAM IT systems.
* Circumventing security controls to allow unauthorized access to EPAM IT systems.
* Going to pornographic or other inappropriate Internet sites.
* Using EPAM IT resources for unauthorized, personal or illegal activities.

**7.10          Housekeeping**

**Do you periodically clean up your workstation?**

Delete files, particularly sensitive information, that you no longer need. They take up space and use network resources unnecessarily. Be aware that the information can be compromised if information is not carefully deleted.

# 8. Prepare for Quiz

**Now it’s time to see if you have understood the IT Security and Awareness training material and can apply it correctly.**

**There may be multiple correct choices for the questions. Please always select the most suitable answer(s).**

#### 1. What security measures help to protect against the theft of confidential information?

There may be multiple choices for the answers. Please always select the most suitable answer(s).

a. Passwords

b. Encryption

c. Do not use or have access to confidential information.

#### 2. If your computer is behaving strangely, or you think it was used without your permission, what do you do?

There may be multiple choices for the answers. Please always select the most suitable answer(s).

a. Contact the EPAM Support Team.

b. Contact the EPAM IT Security Department.

c. Ignore this case.

#### 3. What emails are suspicious?

a. Those that contain the following attachments: \*.exe, \*.bat, \*.com, \*. scr.

b. The subject line is strange or unusual.

c. I do not recognize the sender.

d. It is not work-related.

e. All above.

#### 4. New employees must first…

a. Ignore policies that do not concern them.

b. Read and accept the EPAM Policies.

#### 5. If you go to lunch or leave your workplace, what do you need to do before leaving?

a. Inform my colleague that I am leaving my workplace.

b. Log off or lock my workstation.

c. Make sure my laptop is locked with a security cable (if one is provided to you).

d. Put confidential documents in a secure place (if any).

e. All of the above.

f. None of the above

#### 6. Where do you store confidential documents?

a. Copy the files to a pendrive.

b. Leave sensitive data on the desk.

c. Ask the Project Manager for the secure internal (Confluence/KB/Sharepoint, etc.) or external (Office365) resources.

#### 7. Which of the following are necessary to create a strong password?

a. Mixed-case letters, numbers, punctuation, and special characters.

b. Keep it easy to remember and hard to guess.

c. Make it at least 9 characters long and change it at least every 3 months.

d. Do not use proper names or dictionary words (in any language).

e. Do not use the same password for all systems you access.

f. Memorize it and keep it a secret, do not share it with anyone.

g. All above.

#### 8. Is it prohibited to connect personal Wireless Access Points to the EPAM network?

a. Yes.

b. No.

#### 9. As an authorized remote access user, take the necessary steps to:

a. Keep your password a secret, even from family members.

b. Keep your antivirus software up to date.

c. Check if your computers have the required software updates installed on them and patches are up to date.

d. Workstation firewall is turned-on.

e. All of the above.

#### 10. To prepare for the unexpected:

a. Save new documents immediately.

b. Set your PC to save automatically every 5-10 minutes.

c. Save important files to a server that is backed-up on a daily basis.

d. All of the above.

#### 11. What are the security requirements of using a corporate laptop?

a. When in the office, laptops should be secured to an immovable object with a computer security cable.

b. Log off or lock your laptop when leaving it unattended.

c. Do not leave your laptop unattended in an open freely accessible area even if the laptop is locked with a security cable like a. ‘Kensington lock’.

d. All of the above.

#### 12. What kind of software can you install on your workstation?

There may be multiple choices for the answers. Please always select the most suitable answer(s).

a. Any software.

b. EPAM software packages.

c. Software that is authorized by WFT License Management Support Team. (The request should be issued via support.epam.com)

#### 13. How can you protect your computer against viruses?

a. I keep antivirus software up-to-date on my computers.

b. I don't open suspicious email or instant messenger attachments.

c. I download any type of programs only from trusted Internet sources.

d. All of the above.

#### 14. Which Data Privacy and IT Security directives should be followed if you work from Customer premise?

a. Work as you usually do in an EPAM office.

b. Just follow the Customer’s rules.

c. Always follow the strongest rules, no matter where it originates from (EPAM or the Customer).

#### 15. Can you use Web-based services (e.g. Dropbox, etc.) for storage of and collaboration on company content?

a. Yes.

b. No. This is strictly forbidden by Company policy.

#### 16. Under company policy, which of the following are allowed for storing project-related information? Please choose the correct answer(s) from the below list:

a. We have an enterprise subscription for Office 365 products.

b. OneDrive for Business for document sharing and collaboration

c. Office Online applications (Word, Excel, PowerPoint, OneNote)

d. Information Rights Management solution based on Microsoft Azure RMS.

e. All of above.

f. None of the above.

#### 17. What should you do if you receive an email - even from a @epam.com user - asking you to update your EPAM account by clicking a link?

a. Follow the instructions and click on the link.

b. Recognize that it is a suspicious email and immediately delete then inform support@epam.com about this potential phishing e-mail.

#### 18. Usage of Torrent / Peer-to-peer software is strictly forbidden due to the following risk(s):

a. They are safe carriers for botnets

b. They expose endpoints which were otherwise behind a Firewall and not visible to the outside world directly to the internet.

c. They provide cover for malware to hide in the network and ex-filtrate critical organizational information.

d. They run unchecked in the enterprise.

e. All of the above.