european informatics passport

# IT SECURITY

## Syllabus

certipass

SYSTEM CERTIFICATION ISO 9001 SGS

ACCREDIA L'ENTE DI ACCREDITAMENTO

## Disclaimer

Certipass has produced this document on topics related to digital culture and improved computer use, based on standards and references applicable to these subjects. Due to the complexity and enormity of the subject, however, Certipass as a publisher cannot guarantee the total comprehensiveness of the information provided. It cannot be held responsible for any eventual errors, emissions, losses or damages caused by this information, instruction or advice contained within the publication and eventually used by third parties.

Certipass reserves the right to make any changes or corrections at its own discretion at any point, without prior notification.

The user is obliged to obtain information regarding modifications from eipass.com, in the dedicated Programme area.

## Introduction

Competition, innovation and social cohesion increasingly depend on the strategic and effective use of new information and communication technologies. This requires competence, creativity, and awareness on the part of those who use ICT tools every day.

Obtaining and certifying these skills through a recognised, objective system facilities mobility. A commonly-accepted 'language' in this sector provides the opportunity for everyone to think about their own ICT competence, and, more importantly, to display these skills on their CV. When applying for jobs this gives candidates something extra, something that employers are undoubtedly looking for. The skills outlined in this document represent a 'structure' for defining e-competence that could be transferred onto the Europass Curriculum. *From the Introduction to e-Competence Framework for ICT Users.*

The e-Competence Framework for ICT Users was developed by CEN, the European Committee for Standardisation, based on a series of EU rules and policies, including:

- European e-Skills Summit Declaration;
- Decision 2318/2003/EC by the European Parliament and Council to adopt a multiannual programme for the effective integration of information and communication technologies (ICT) in education and training systems in Europe (eLearning Programme);
- e-Skills in Europe: Towards 2010 and Beyond. A summary of the European e-Skills Forum report presented at the European e-skills Conference;
- European Commission communication on e-Skills in the 21st Century: Fostering Competitiveness, Growth and Jobs;
- Digital agenda for Europe.

The e-competence framework provides an overall outline of the digital skills that an average user of computers, the internet and new information and communication technologies should possess. **The use of a shared language to describe skills and proficiency levels makes it easily understandable throughout Europe and beyond.** The tool was created to facilitate the immediate assessment of IT skills in varying environments and for different groups of people. These include students, employees, managers, Human Resource departments, those working in educational institutions, policy makers and those in the public sector.

Our **User Programme** makes direct reference to classifications provided by the **e-Competence Framework for ICT Users (e-CF)**, making it relevant and applicable in all sectors: it is the first programme of its kind to make full use of the framework's structure, rather than simply replicating the principle ideas. The **User Programme**, more precisely, assesses and certifies intermediate ICT skills, as described in the summary table of the **e-Competence Framework for ICT Users – Part 2: User Guidelines**.

The **User Programme** is a great way to objectively demonstrate the ability to correctly and maturely use ICT tools in a school or university environment, at work, or on a personal level.

**The programme takes into account the independent nature of different software and hardware producers, and fulfils all criteria for interoperability and neutrality.**

*Study Center* EIPASS

## Our method

Going beyond the tired ‘explanation, activity, test’ method, we propose a new way to link and describe the content of the modules, based on that used in the **e-Competence Framework for ICT Users – Part 2: User Guidelines**.

The programme is the obvious choice for those who need to build their ICT skills and obtain a certification. For every topic, we have provided a reference framework which consists of:

- a basic definition of the skill;
- everything the User must know in about the topic, the theory or *knowledge*.
- the *skills* related to the aforementioned theory that a certified User must possess.

## Procedures and tools

In order to prepare for the test, the candidate has full access to the online training and support available in your reserved area on DIDASKO platform.

To pass the exam, the candidate must be able to correctly answer at least 75% of the 30 questions for each module. The idea is that every module represents a specific skill. Due to the links between these skills, the candidate is free to choose the order in which they want to move through the modules.

MODULE

# IT SECURITY

## What does a certified EIPASS User know how to do?

A certified User understands the concept of IT security, the difference between active and passive security and how to recognise an attack by a hacker

He/she is aware of the most widespread malware and know how to protect appliances and data against it. He/she understands the importance of ensuring data is authentic, credible, intact and confidential and knows how to back them up and recover them.

He/she can safely use emails and online communication tools and knows how to use P2P technology correctly. He/she knows how to browse safely, taking all precautions to look after ones own data.

## Contents of the module

**Definitions**

- The purpose of IT Security
- The concept of privacy
- Measures for file safety

**Maleware**

- Defence tools
- Heuristics

**Network safety**

- Network and connections
- Browsing safely on wireless networks

**Browsing safely**

- The browser and online security
- Tools provided by Google Chrome
- Content-filtering tools

**Safe online communication**

- The vulnerability of email
- How to manage online communication tools
- Peer-to-peer technology

**Data security**

- Running a PC in a safe way
- System recovery
- Permanently deleting data

# 1 | DEFINTIONS

The User knows about the role and the importance of IT Security in day-to-day digital life. He/she can identify various hacker profiles and understand the significance of IT crime. The User knows the difference between passive and active security measures, and about the concept of social engineering. He/she knows how to apply security measures to Office files.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **1.1** | The purpose of IT Security | **1.1.1** | Define the concept of *IT security*, understanding the difference between *data* and *information* and knowing security standards and how to certify them (ISO) |
| | | **1.1.2** | Define the risk of the equation between threat/ vulnerability and countermeasures; define the central aspects of *IT Security*: integrity, confidentiality, availability, non-repudiation and authentication |
| | | **1.1.3** | Explain threats and how to distinguish them from accidents and unwanted events |
| | | **1.1.4** | Understand the meaning of *IT crime* and recognise the different types of *hacker* |
| | | **1.1.5** | Distinguish between passive and active measures |
| | | **1.1.6** | Identify and activate security measures, including authentication and the use of a proper password for every account, the use of OTP, two-factor authentication (through SMS and email, applications and one-button authentication), cancellation of data of browser history; understand and define biometrics when applied to IT security; define the concept of accountability |
| **1.2** | The concept of privacy | **1.2.1** | Recognise the problems connected to the security of personal data |
| | | **1.2.2** | Define the concept of *social engineering* |
| | | **1.2.3** | Understand the concept of IT theft and what it entails; use good practice for limiting danger; assess whether one's identity has been stolen, and, if necessary, know who to talk to and what to do to limit damages |
| | | **1.2.4** | Understand how to defend oneself from social engineering |
| **1.3** | Measures for file safety | **1.3.1** | Define a macro and understand the implications with regards to security |
| | | **1.3.2** | Change the macro settings in the *Security Centre* |
| | | **1.3.3** | Set a password for Office files |

## 2 | MALWARE

The User knows about the most widespread and the latest malware, built on the principle of heuristics. He/she knows about the most popular protection measures (above all, antivirus) and knows how to use them in an appropriate way, to effectively protect appliances and data from external attack.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **2.1** | Malware | **2.1.1** | Define the concept of malware, differentiating between parasite types and those from the start-up sector |
| | | **2.1.2** | Identify and define the most widespread malware: virus, worm, trojan horse, dialer, hijacking, zip bomb, spyware; identify the most dangerous spyware (phishing, vishing, pharming, sniffing); recognise the way malware is spread; understand if one's PC has been infected with spyware; avoid being infected by spyware and in the eventuality, remove it |
| | | **2.1.3** | Define and recognise the function of malware *attacks using login information*: thiefing and keylogger |
| **2.2** | Defence tools | **2.2.1** | Explain the concept of a Firewall: what it is for, how it works on a technical level; the different types |
| | | **2.2.2** | Explain what antivirus is for |
| | | **2.2.3** | Explain how antivirus works and what it is made up of |
| | | **2.2.4** | Define the different options available to run a system scan; understand the concept of advancement and the analysis of scan results, define real-time and behaviour analysis, recognise the different types of repair |
| | | **2.2.5** | Assess the importance of constantly updating antivirus systems; define the concept of heuristics applied in this context, define a CERT (Computer Emergency Response Team) |
| **2.3** | Heuristics | **2.3.1** | Define the concept of heuristics and explain how malware works according to its principles |

## 3 | NETWORK SECURITY

The User knows how to manage authentic, credible, whole and secure data and knows how to back them up, recover them and send them, using all the appropriate ways to guarantee their security. He/she knows the function of a wireless network and the most-used protocols for protecting this type of network and recognise the dangers connected to browsing on public networks.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **3.1** | Network and connections | **3.1.1** | Define the concept of *networks* and networking |
| | | **3.1.2** | Distinguish between the different network types (LAN, WAN and MAN) |
| | | **3.1.3** | Distinguish between the different types of LAN networks (star, bus, ring, mesh) |
| | | **3.1.4** | Understand the principles of network vulnerability, recognising the different types |
| | | **3.1.5** | Identify the roles and responsibilities that a system administrator has with regards to network security |
| | | **3.1.6** | Explain why a firewall is useful and how it works from a technical perspective; distinguish the firewall from its inner workings (from filtering packs and on a circuit level) |
| **3.2** | Browsing safely on wireless networks | **3.2.1** | Understand the importance of using passwords for Wi-Fi access |
| | | **3.2.2** | Identify different protocols for protecting this type of network: WEP (Wired Equivalent Privacy, WPA (Wi-Fi Protected Access) and WPA 2 (with Advanced Encryption Standard) |
| | | **3.2.3** | Explain how a hotspot works; how to activate a personal hotspot or tethering; how to connect and disconnect through a hotspot; how a hotspot 2.0 works and how to activate it on Windows 10; recognise the difference between a hotspot and a hostpot 2.0; explain the concept of roaming |
| | | **3.2.4** | Recognise the dangers of browsing on public wireless networks |
| | | **3.2.5** | Explain the different types of attack on public wireless networks: interception or eavesdropping, jamming and MITM (man-in-the-middle attack) |

## 4 | BROWSING SECURELY

The User will learn about and apply measures to ensure safe and secure browsing. He/she will understand how to activate security measures in Google Chrome. He/she will learn the features of specific software for filtering content and for safe browsing.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **4.1** | The browser and online security | **4.1.1** | Explain the concept of temporary internet files: what they are and how to manage them |
| | | **4.1.2** | Save passwords for different accounts; understand the advantages and the disadvantages of saving passwords on a PC and of deleting memorised passwords |
| | | **4.1.3** | Set-up, use and delete the automatic data fill-in function on online forms |
| | | **4.1.4** | Define active codes: what they are and how to manage them |
| | | **4.1.5** | Define the difference between session cookies and persistent cookies and their impact on data security |
| **4.2** | Tools provided by Google Chrome | **4.2.1** | Recognise icons relative to the SSL (Secure Socket) protocol, understand the meaning of a security certificate and its function |
| | | **4.2.2** | Manage warnings for insecure sites |
| | | **4.2.3** | Explain Sandboxing: what it is and how to manage it |
| | | **4.2.4** | Explain automatic updates |
| | | **4.2.5** | Explain Smart Lock: what it is and how it works |
| | | **4.2.6** | Browse incognito and set preferences |
| | | **4.2.7** | Explain how to protect privacy, browsing incognito and managing the appropriate preferences |
| **4.3** | Content-filtering tools | **4.3.1** | Understand the function of the browser filter system; how to manage SafeSearch in Google Chrome: activate, deactivate and block filters |
| | | **4.3.2** | Report inappropriate images and sites |
| | | **4.3.3** | Recognise the functionality of Google's online security centre |
| | | **4.3.4** | Identify and define Window's Safety Family |
| | | **4.3.5** | Explain how Homeguard Activity Monitor and other content-filtering software works. These include K9 Web Protection, Qustodio Free and SocialShield |

## 5 | SAFETY IN ONLINE COMMUNICATION

The User knows how to use emails, chat, instant messaging and social networks safely and securely and to understand and correctly use P2P technology.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **5.1** | The vulnerability of email | **5.1.1** | Understand and distinguish between different threats; understand the purpose of email encryption; recognise, define and use software to encrypt email messages: Virtru, ProntonMail, Sbwave Enkryptor, Lockbin, Encipher.it, Secure Gmail |
| | | **5.1.2** | Explain digital signatures: what they are, the difference between a digital signature and email encryption |
| | | **5.1.3** | Define the characteristics of phishing and recognise fraudulent emails that aim to steal information; what to do if he/she becomes a victim of phishing |
| | | **5.1.4** | Explain how to manage unwanted emails or spam; what to do to reduce the risk of being spammed |
| | | **5.1.5** | Securely run a Gmail system: create and update the password, verify unauthorised access, mark mail as phishing or spam, mark mail previously marked as spam as normal, add or update an anti-spam filter |
| **5.2** | How to manage online communication tools | **5.2.1** | Identify and manage the possible risks that come with using a blog, instant messaging and social networks (Facebook and Twtter), including grooming and improper disclosure of images |
| | | **5.2.2** | Identify cases of social network poisoning and understand the potential and grave dangers that come with unethical social network use, such as cyberbullying |
| | | **5.2.3** | Use software that consents to safe sharing of messages and their content (ChatSecure, Silent Circle, Signal Messenger, Telegram, Wickr) and understand and describe the content of end-to-end encryption |
| **5.3** | Peer-to-peer technology | **5.3.1** | Understand and define the features of P2P applications, being aware of the security and copyright implications. |
| | | **5.3.2** | Understand and assess the practical risks that come with P2P: malware, pirated software, system slowdown |

## 6 | DATA SECURITY

The User knows how to manage his/her PC so that it does not house bugs, understands the concept of storage and recognises the key kinds (NAS, DAS and SAN), understands the concept of backup and how to do it on both a Windows and Mac, understands how it can be done on the cloud and how to recover the system. He/she knows how to delete files completely from the PC.

| Knowledge | | Skills | |
|---|---|---|---|
| A certified User knows about... | | A certified User can... | |
| **6.1** | Running a PC in a safe way | **6.1.1** | Identify and define storage; distinguish between advantages and disadvantages of the principle types: NAS (Network Attached Storage), DAS (Direct Attached Storage) and SAN (Storage Area Network) |
| | | **6.1.2** | Explain Backup: what it is, what it’s for, how to undertake a manual backup, understand the advantages of completing a backup using *Windows 10 file history*; recover saved files |
| | | **6.1.3** | Recover saved files and exclude files from the backup if they are no longer needed |
| | | **6.1.4** | Backup a Mac, using Time Machine |
| | | **6.1.5** | Explain the cloud and how OneDrive works; recognise and use specific software for backups |
| **6.2** | System recovery | **6.2.1** | Explain system recovery: what it is and how to do it on Windows 10 |
| | | **6.2.2** | Perform a system recovery on a Mac |
| **6.3** | Permanently deleting data | **6.3.1** | Explain the recycle bin: what it is and how it works |
| | | **6.3.2** | Know the specific software which allow permanent deletion of files |

ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE EIPASS

certipass

- ACCREDIA CERTIFICATION BODY, PRS N.116C
- PROVIDER OF INTERNATIONAL DIGITAL SKILLS CERTIFICATION PROGRAMS EIPASS
- ACCREDITED BY THE MINISTRY OF EDUCATION IN PROFESSIONAL CONTINUING DEVELOPMENT FOR THE ACADEMIC STAFF (DIR. 170/2016)

FOR INFORMATION ON IT CERTIFICATIONS

**en.eipass.com**
**contact@eipass.com**