RULES AND POLICIES

The full text on rules and policies can be found in Yammer (https://www.yammer.com/ie.edu/), in the Information Security Group.

Please, be sure to check the following content:

- Scope
- Technical support and help
- Security on computers, mobile devices and data
- Personal data
- Systems use policy
- Software
- Hardware
- Remote access to IE
- Electronic mail
- Standards to minimize the network traffic
- Rules relating to physical security and supports

The Information Security Office is available for any questions or reports of security incidents via:

Information.Security.Officer@ie.edu

CONTACT US

Information.Security.Officer@ie.edu

https://servicedesk.ie.edu

Cybersecurity

Policies and Standards

IE INFORMATION SECURITY POLICY: SUMMARY AND STANDARDS FOR IE AND IEU STAFF

PASSWORD:

Memorize your password.
Do not write it down or share it with anyone. Change it regularly, every three months at the least.

CORPORATE DEVICES:

• It is forbidden to modify the initial settings of all IE devices.

• Do not authorize anyone to use your IE computer without your supervision.

• Downloading and installing software is forbidden. If you wish to install specific software, please contact the IT Service Desk with the request.

• Do not modify or disable any security option or default applications from your IE computer and/or mobile.

• Block access to devices when not making use of them. On a PC, use the Ctrl-Alt-Del key combination.

• Immediately report to IT any theft or loss of your laptop, smartphone, memory card or other mobile data storage device.

• Back up your data regularly. You may do so manually or using the Bytepass application installed on your PC.

• When receiving an alert from the Antivirus tool, contact Service Desk indicating it's a matter of urgency, and wait for them to come back to you with a solution.

PERSONAL DEVICES:

To connect to the IE corporate network -including the IECorp WiFi- with your personal devices (computers, tablets and smartphones), these must meet the following standards and requirements:

• Have an antivirus and personal firewall activated. The installation and maintenance of these tools need to be done by you. If the devices do not meet these requirements, IT may deny you access to the network.

• You are responsible for backing up corporate data on your personal devices.

• When receiving an alert from the Antivirus tool, contact Service Desk indicating it's a matter of urgency, and wait for them to come back to you with a solution.

PERSONAL DATA:

The creation of files containing personal data, will require notification to information security office (CISO) or legal department, in compliance with the data protection act, to assess your request and, if necessary, apply for the registration in the Spanish Agency of Data Protection, and deploy the rest of legal requirements (it does not include files of personal contacts: friends, family, etc.)

PERSONAL USE:

Personal use of IE corporate systems and devices is permitted, provided that it does not interfere with work or involve the installation of any additional software or hardware on the computer since this could damage the configuration and interfere with the use of professional tools.

Personal data or files stored in an IE corporate computer must be properly identified, stored in a folder called PRIVATE.

RULES RELATING PHYSICAL SECURITY:

Any documentation or media containing data of a personal nature must be destroyed: Paper documents must be shredded and pen-drives must be formatted.

• Have an antivirus and personal firewall activated. The installation and maintenance of these tools need to be done by you. If the devices do not meet these requirements, IT may deny you access to the network.

• You are responsible for backing up corporate data on your personal devices.