Security in companies and own business – work environment, company emails and communication & Map of European Union IT Security Rules

Co-funded by the
Erasmus+ Programme
of the European Union

Lithuanian gymnasium team

What is Workplace Security?

It is basically the process to protect an employee from work related illness and injury and to make the workplace secure from intruders.

Every company should have an Environmental, Safety and Health Policy statement, in other words, a workplace safety plan

Emails Are For Business Use

Though it may seem obvious, your policy should be clear that the use of a business email address is for business only. You may draw a distinct line that any personal use of business email is strictly prohibited, or your policy could include guidelines on how to handle personal email because there are times when a personal matter might be discussed on a business email account.

Emails Are Company Property

Along the lines of “business email is for business use,” your policy should make it clear to your employees that all company email is the company’s property. That is, any email that is sent, received, created, or stored on a company’s computer system may be viewed and even admissible in a legal case.

Company Network and Security

One of the most important things your email policy should address is security because emails provide a perfect opportunity for security breaches. Phishing and, more specifically, spear phishing emails have increased and are common cyber-attacks on small businesses.

Cybersecurity in Europe: stronger rules and better protection

The European Union is strengthening its cybersecurity rules in order to tackle the increasing threat posed by cyber-attacks as well as to take advantage of the opportunities of the new digital age.

In parallel, the EU is working on cross-cutting measures which tackle cyber threats in several areas.

- **fight against organised crime** - where cybercrime is listed among the top 10 priorities for the 2018-2021 period
- **common foreign and security policy** - where deterring cyber-attacks is important to achieving the CFSP objectives
- **cyber defence** - where the EU has updated its framework taking into account the changing security challenges

Why do we need it?

Faced with ever-increasing cybersecurity challenges, the EU needs to improve awareness of and the response to cyber-attacks targeting member states or EU institutions.

These challenges stretch across national and EU borders and impact not only security and stability but also our very prosperity and democratic order.

Some Lithuanian laws restricting online activity

- Every person shall have the right to freely express his ideas and convictions and to collect, obtain and disseminate information and ideas unless it is necessary to protect the constitutional system, a person's health, honour, dignity, private life and morality.
- In order to ensure freedom of information, it shall be prohibited to exert pressure on the producer or disseminator of public information, their participant or a journalist, compelling them to present information in the media in an incorrect and biased manner.
- In producing and disseminating public information, a person's right to protection of information of private nature must be ensured.