Safety and security policy within EDO and its working units

Introduce:

EDO has the safety and security of the employee above all the concerns, because EDO believes in the value and the right of human in maintaining his safety and security .first of all to preserve his humanity, second to provide security and peace that will provide an encouraging and stimulating work environment for achievement, so EDO has developed a set of procedures and instructions that ensure the safety and security of employees represented in the following:

The occupational safety and security procedures which related with the work environment:

1- EDO specifies security officer for the security inside workplace.
2- It shall not be permitted to leave any materials that could be flammable inside workplace.
3- An alarm system should be put for any emergency call.
4- Emergency action plan to alert employees to workplace emergencies.
5- Training all workers on first aid in case of any emergency until the specialist's arrival.
6- The safety of electricity, gas and other connections shall be verified periodically by the security officer.
7- Provide the workplace with fire extinguishers and put them in accessible places and train employees to use them.

The occupational safety and security procedures which related with Car tracks:

1- Commitment to the speed determined on the road.
2- Commitment to fasten the seat belts.
3- Commitment to not to talk in the phone while driving.
4- Commitment not to talk to guests.
5- Commitment to Car cleanness.
6- In the event of a risk, the driver must contact the following numbers 01282407518 or 01225985529.
7- In case you face a security situation on the road you should refer to the specialist.
8- Commitment to the proper words.

The occupational safety and security procedures which related with Information Security:

1- Periodic monitoring of the Office's equipment, any problems related to the security and of the stored files.
2- Provide another means to save the data of the Office to be used in case of loss of any files or information.
3- Provide original software protection and drivers for office devices as much as possible or provide them for some of the most important hardware.
4- Implement and use the LAN internal.
5- Evaluate the security status of the participating servers to ensure that our data is stored securely.
6- The annual renovations for the encoded certificate https which include encode our data to and from the EDO server to prevent any attempts to access to our data illegal.
7- Awareness of the importance of information security and its seriousness to the institutions of the work team.

Responsibility of individuals within EDO:

Dealing with office hardware

1- Do not disclose the password of the computer to anyone.
2- Ensure that no one uses your own device, specially the visitors and the volunteers and in necessary case you should go to the administrator and be under supervision.
3- Save a copy from the important data and files on external hardware because it allows you to restore any data when you lose it and the IT unit will provide a way to back up your files.
4- It is forbidden to Put any unauthorized software or use it before you refer to the manager.

Dealing with the official e-mail of the office:

The employees should follow these procedures:

1- Ensure that you singed up from the e-mail after you finish.
2- Delete unnecessary message.
3- Delete any unknown text message which requested personal information and avoid clicking on links in text messages.

The employees are forbidden from:

1- Sending e-mails or forwarding a message containing slander, assault or racism. If you receive an email of this kind, you must immediately notify the administrator.
2- Sending unauthorized messages (you should write an address for messages so they do not reach to the recipient as a spam.
3- Disclose their passwords to anyone.
4- Allow anyone to use the employee's email.
5- Open a message with a strange address.
6- Respond to messages that ask you to fill in your username and password.
7- Use the mail for purchases of work supplies without previous permission.
8- Use the e-mail for personal purchase.
9- Use the e-mail on your personal mobile for opening Social Media (Facebook or whatsapp).
10- Use the office email to subscribe to any program or application without permission from the specialist.

Dealing with the Internet and websites:

1- Do not disclose the password of your online account to anyone.
2- Do not open any public Wi-Fi networks as much as possible from the office devices.
3- Check the sites that are accessed and do not open any untrusted links.
4- You cannot register on any site by the email of office.

Office management