TIP SHEET SERIES **NO. 17**

Physical Security is a part of our life!

Physical security violations can create more problems for an organization than virus attacks. Loss of data, shutdown of systems or arson can cause long-term and serious damage to institutions. Thus, it is important to consider physical security and know how to provide it.

- **Backup the Data.**

  Backing up important data is an indispensable part of recovery in case of emergency, but it should be noted that the information on these backup tapes, disks can be stolen and used by someone outside the company.

- **Lock the server room.**

  Set policies that require these doors to be locked when the server room is empty. Determine who should have the keys to the server room. The server room is the heart of physical network, and a person who can physically access the servers, switches, routers, cabling, and other devices in that room can do great harm. For this reason, necessary precautions should be taken.

- **Put important and vulnerable devices in a locked and secure room.**

  A hacker can plug a laptop into a hub and use certain software to grab outgoing data on the network. Put as many of your network devices as possible in a locked room. If your devices need to be in a different area, be sure to lock them somewhere else. Hackers can use any unsecured computer connected to the network to access or delete information that is important to your business. Computers in vacant offices or in places where people outside can easily access, such as a reception desk, are particularly vulnerable. Equip the computers that need to stay in the open space with smart cards or biometric readers.

- **Cameras should be positioned to the necessary places.**

  Knowing who goes in and out of the organization is also important in terms of physical security. In cases where the camera is secretly installed, the cameras will also help to see who has entered and exited. Cameras can use motion detection technology, which records when someone is on the move. In case of motion detection, they can be set to send email or mobile phone notifications.

- **Disable the drivers.**

  Employees can copy company information to removable drives. If you do not want this, you can disable or completely remove floppy drives, USB ports, and external drive connections.

- **Protect portable devices.**

  Laptop computers and handheld computers pose significant risks in terms of physical security. If employees use laptop computers at the desk, they must take them with them when they leave or lock them with a cable.

- **Natural disaster policies and procedures and providing security in such cases.**

  What should be done to get rid of natural disasters? Testing this question is another way of ensuring physical security.

- **Protect your printer.**

  Most modern printers keep document content in their internal memory. A hacker steals the printer and gets its memory, he/she can obtain copies of the documents that were printed recently. Printers, such as servers and workstations that store important information, should also be located in safe locations and be set at a certain point so that they can not be moved.