# User management

CH5

# 5.1 Issues

- User management is about interfacing humans to computers.
- This brings to light a number of issues:
  - Accounting: registering new users and deleting old ones.
  - Comfort and convenience: making the system easy to use and navigate.
  - Support services: providing assistance to users as needed.
  - Ethical issues: such as data privacy and confidentiality.
  - Trust management and security: ensuring the security and safety of user data.
- Some of these (account registration) are technological, while others (support services) are human issues.
- Comfort and convenience lies somewhere in between.
- User management is important because the system exists to be used by human beings, and they are both friends and enemies.

# 5.2 User registration

- One of the first issues on a new host is to issue accounts for users.
- For small organizations, user registration is a relatively simple matter.
- Users can be registered at a centralized location by the system manager, and made available to all of the hosts in the network by some sharing mechanism, such as a login server, distribute authentication service, or by direct copying of the data.
- For larger organizations, with many departments, user registration is much more complicated.
- It is convenient for autonomous departments to be able to register their own users, but it is also important for all users to be registered under the umbrella of the organization, to ensure unique identities for the users and flexibility of access to different parts of the organization.

# 5.2 User registration

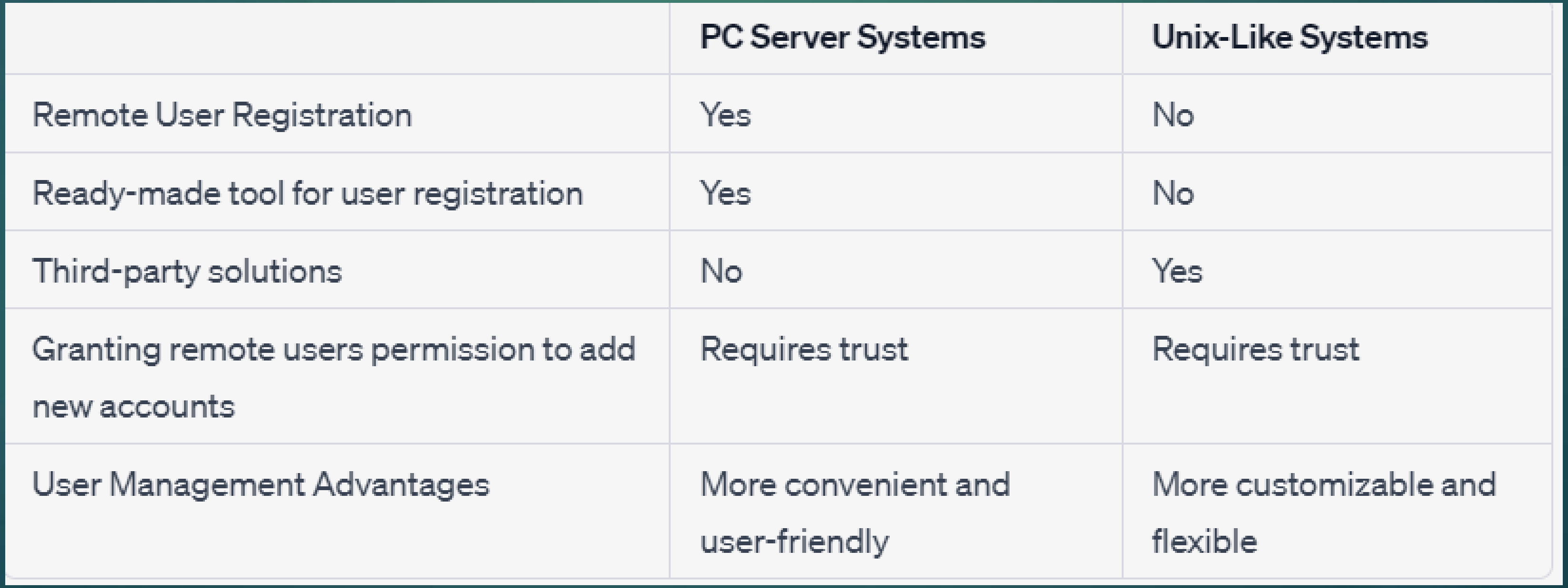
- PC server systems like NT (Windows NT) and Netware are network operating systems designed to run on PC-based servers. These systems offer a range of features and capabilities, including user management, file and print sharing, application services, and network security.
- Windows NT was first released by Microsoft in 1993 and was designed to be a high-performance, multi-user operating system. It was built to support client-server computing. NT offered advanced features such as support for multiple processors, a powerful security model, and a flexible file system.
- NetWare, on the other hand, was developed by Novell in the 1980s and was designed to be a powerful network operating system for business use. It offered a range of advanced features such as support for multiple network protocols, file and print services, and advanced security features.
- Both NT and NetWare have been widely used in enterprise environments for many years, and both offer powerful user management capabilities. These systems have been used to manage large numbers of users and devices on complex networks, and they have played a key role in the development of modern enterprise computing. However, with the rise of cloud-based systems and other modern technologies, the role of these systems has evolved, and many businesses are now looking to newer platforms for their network management needs.

Image of a PC server

# User Registration in NT

PC server systems like NT and Netware have a significant advantage in user management over Unix-like systems.

One advantage of PC server systems such as NT is the ability to register single users remotely. This is done by using the command "net user username password /ADD /domain" from a workstation. This feature provides convenience and reduces the need for physical access to the server.



| | PC Server Systems | Unix-Like Systems |
|---|---|---|
| Remote User Registration | Yes | No |
| Ready-made tool for user registration | Yes | No |
| Third-party solutions | No | Yes |
| Granting remote users permission to add new accounts | Requires trust | Requires trust |
| User Management Advantages | More convenient and user-friendly | More customizable and flexible |

# 5.2 User registration

- Unix-like systems offer shell scripts or user interfaces for user management, but these may not be suitable for all organizations.
- Default system layouts may not align with an organization's specific needs, making some of these scripts or interfaces unusable in a network environment.
- Assigning new user accounts on Unix-like systems can pose security concerns since granting remote users the ability to add new accounts must be done with caution.
- As a result, many organizations opt for third-party solutions to address these challenges and manage their user accounts more effectively.
- Using such solutions can help organizations customize their user management processes, ensure network security, and meet their specific needs.

# 5.2.1 Local and network accounts

- To centralize passwords, most organizations require a system where each user has the same password on each host on the network.
- Both Unix and NT allow the creation of accounts locally on a single host, or 'globally' within a network domain.
- Local accounts only grant permission to use the local host, while network accounts enable users to use any host within a network domain.
- Local accounts are configured on the host itself, while Unix registers local users by adding them to the files /etc/passwd and /etc/shadow.

# 5.2.1 Local and network accounts

- Sun Microsystems' Network Information Service (NIS) is a way of managing user accounts and passwords in Unix-like systems. Users are registered locally on a central NIS server, but there is no way to register or manage users remotely. NIS is useful for sharing passwords across a network, but it has security implications. Encrypted passwords are distributed in an old, visible format that can be seen by anyone on the network. This makes shadow password files, which are supposed to securely store encrypted passwords, ineffective at protecting password security.
- NIS can be a convenient way to manage passwords across a network, but it can also create security vulnerabilities.

# 5.2.1 Local and network accounts

- Windows NT (NT) uses the Security Accounts Manager (SAM) as its user registration mechanism.
- Users registered in the SAM of a primary domain controller are registered within that domain and can access any host that subscribes to that domain.
- NT domains involve shared databases, administrative policies, and security models.
- To ensure secure communication and a distributed user environment, NT uses two technologies: Kerberos and the Open Software Foundation's Distributed Computing Environment (DCE).
- Kerberos is used to authenticate users and provide secure communication over a network.
- DCE provides a distributed computing environment that allows users to access resources from any machine in the network.
- Overall, NT's SAM mechanism and its use of Kerberos and DCE help to ensure secure user authentication and communication in a distributed computing environment.

# 5.2.2 Unix accounts

- To add a new user to a Unix-like host, several steps need to be taken.
- The first step is to find a unique username, user-id (uid) number, and password for the new user.
- Next, the system database of user accounts needs to be updated. For Unix, this means adding a line to the file /etc/passwd (or on the centralized password server of a network) for the new user.
- A login directory (home directory) needs to be created for the user.
- A shell needs to be chosen for the user, if appropriate.
- Finally, some configuration files like .cshrc or .profile need to be copied into the new user's directory, or the system registry needs to be updated.

# 5.2.2 Unix accounts

- Unix developers have created three different password file formats which increase the awkwardness of distributing passwords.
  - The traditional password file format is the following:
    - mark:Ax7Wc1Kd8ujo2:123:456:Mark Burgess:/home/mark:/bin/tcsh
- Username: a unique identifier for the user (up to eight characters)
- Encrypted password: a hashed version of the user's password
- User ID: a unique number that represents the user and is equivalent to the username
- Default group ID: a unique number that represents the default group of users to which this user belongs
- GECOS field: typically the full name of the user, but on some systems can include additional information like office, extension, and home phone number
- Home directory: the root directory for the user's private virtual machine
- Default shell: the command interpreter that's started when the user logs in

The actual password is stored in a separate file, usually **/etc/shadow**, in a hashed form.

# 5.2.2 Unix accounts

- *Shadow password files*
- The format of the password file is then the same as the traditional format , except that the second password field contains only an ‘x’, e.g.:
- mark:x:123:456:Mark Burgess:/home/mark:/bin/tcsh
- There is then a corresponding line in /etc/shadow with the form or with an MD5 password hash.
- Example: mark:Ax7Wc1Kd8ujo2:6445::::::
- The shadow file is not readable by ordinary users and contains many reserved fields for password aging and expiry mechanisms.

# 5.2.2 Unix accounts

- The third form of password file is used by the BSD 4.4 derived operating systems.
- mark:Ax7Wc1Kd8ujo2:3232:25::0:0:Mark Burgess:/home/mark:/bin/tcsh
- It has extra fields which are not normally used, such as a timestamp for the last password change.
- These systems also have an optimization: in addition to the master password file base, they have a compiled binary database for rapid lookup.
- Administrators edit the file /etc/master.password and then run the pwd mkdb command to compile the database which is actually used for lookups. This generates text and binary versions of the password database.

# 5.2.3 Windows accounts

- Windows accounts can be added using the command "net user username password /ADD /domain" or through the graphical user interface.
- The Resource Kit package offers additional tools such as addusers.exe, which allows registering lists of users from a standard file format, but at an extra cost.
- By default, Windows users start in the root directory, but it is recommended to create a separate directory such as \users for home directories.
- Network users usually have their home directory on the domain server, which is typically mapped to the drive H:.

# 5.2.4 Groups of users

- Both Unix and NT allow users to belong to multiple groups.
- A group is an association of usernames that can be referred to collectively by a single name.
- File and process permissions can be granted to a group of users. Groups are defined statically by the system administrator.
- On Unix-like systems they are defined in the /etc/group file, like this:
- users::100:user1,mark,user2,user3
- The name of the group, in this case, is users, with group-id 100 and members user1, mark, user2, and user3.
- Unix groups can be created for users or for software that runs under a special user-id.

# 5.3 Account policy

- Policy rules are necessary for directing user behavior and making system guidelines clear.
- Clear rules make system behavior easy to comprehend, and users are more likely to follow them if they understand them, resulting in more predictable behavior. An accounting policy should include:
- Guidelines on what actions users are permitted or prohibited from taking.
- Descriptions of mandatory enforcement measures that users should expect, such as the removal of garbage files.

# 5.3 Account policy

- This is a script that can be used to close Unix accounts by changing the user's default shell in the /etc/passwd file to the script. The script sends an email to the system administrator with information on the last 10 logins, and a message informing the user that their account has been closed due to a vulnerable password. The message also instructs the user to visit the admin office with personal identification to reopen the account. The script then waits for 10 seconds and exits.shell in /etc/passwd to a script such as

```
#!/bin/sh

echo "/local/bin/blocked.passwd was run" | mail sysadm /usr/bin/last -10 | mail sysadm

message=’

Your account has been closed because your password was found to be vulnerable to attack. To reopen your account, visit the admin office, carrying some form of personal identification.’

echo "$message"

sleep 10

exit 0
```

# 5.10 Computer usage policy

- These are some of the elements that should be included in an organization's policy:
- Guidelines on what actions should be taken by all parties in the event of an employee's dismissal.
- Procedures that should be followed in case of a security breach.
- Clear definition of users' responsibilities to the organization.
- Clear definition of the organization's responsibilities to its users.

# 5.10.1 Example IT policy document for a company

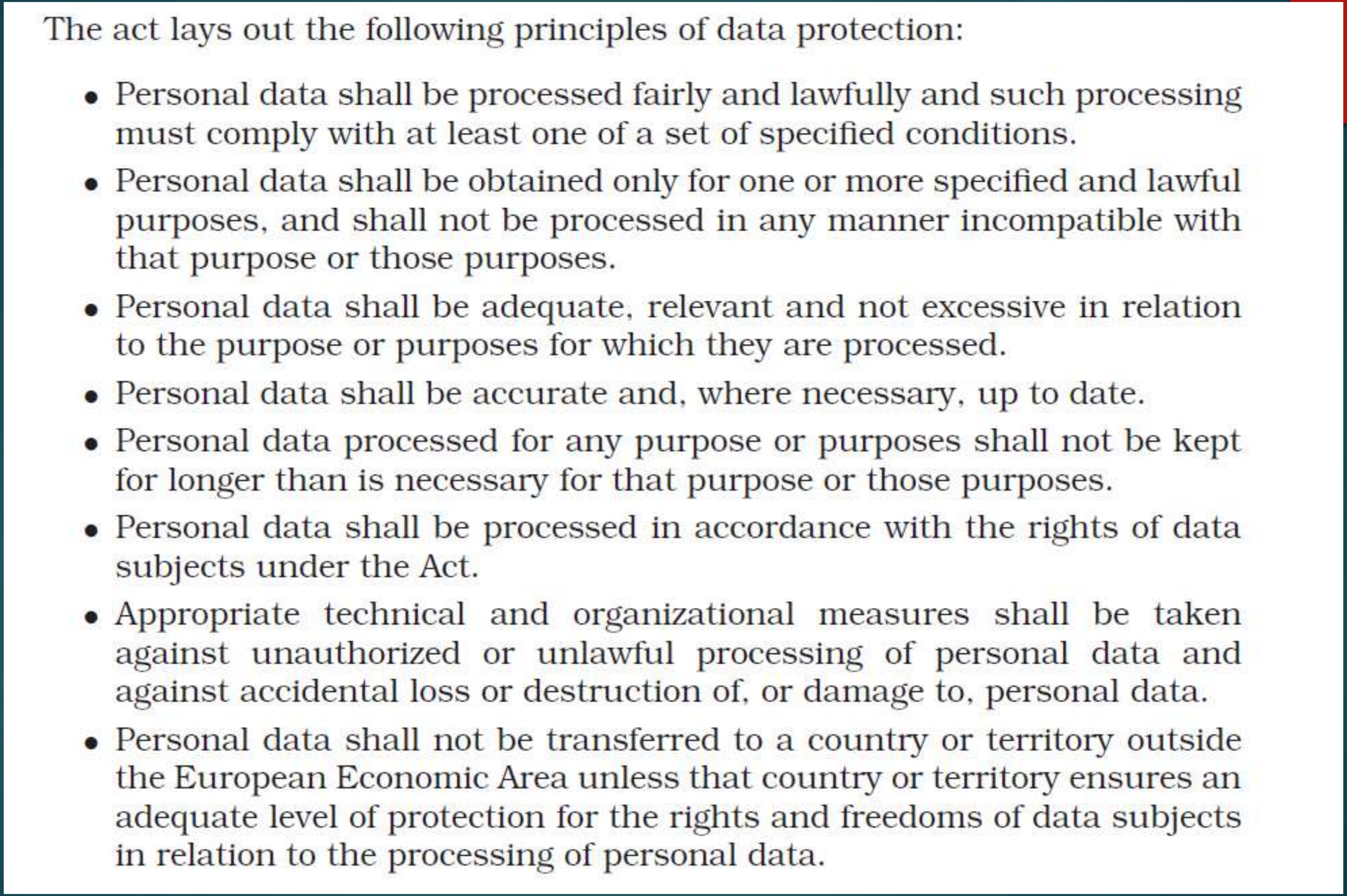
- 1. *Why do we need a policy?*
- As our dependence on technology increases, so do the risks and opportunities for misuse. We are increasingly vulnerable to threats from outside and inside the organization, both due to carelessness and malice.
- From our clients' viewpoint: we need to be perceived as competent and professional in our ability to conduct our business electronically.
- From our company's perspective: we need to maximize the benefits and reduce the risks of using information technology and protect company assets (including reputation)

- 2. *The network*
- The use of the network is not private. The company retains the right to monitor the use of the network by any user, within the boundaries of national law. All users are obliged to use company resources in a professional, ethical and lawful manner.
- 3. *Security*
- Any hardware or software that is deemed a security risk may be disconnected or de-installed at any time, by the system administrator.
- User accounts are set up, managed and maintained by the system administrators.
- Users accessing the network must have authorization by access-rights, password or by permission of the owner of the information.

- Users must take reasonable precautions to prevent unauthorized access to the network. This includes leaving equipment unattended for extended periods while logged on.
- Users must not attempt to gain unauthorized access to restricted information.
- Passwords are provided to help prevent unauthorized access to restricted areas of the network. Users must not log on to any system using another user’s password or account without their express permission.
- Under no circumstances should any user reveal his/her password to anyone else, even by consent.
- Users have a responsibility to safeguard passwords. They must not be written down on paper, stored unprotected online, or be located in readable form anywhere near a network terminal.

- 4. *Copyright*
- Copyright is a statutory property right which protects an author’s interest in his or her work. The right exists as soon as the work is created and continues to exist for the lifetime of the author and beyond, during which time the owner of the copyright may bring actions for infringement.

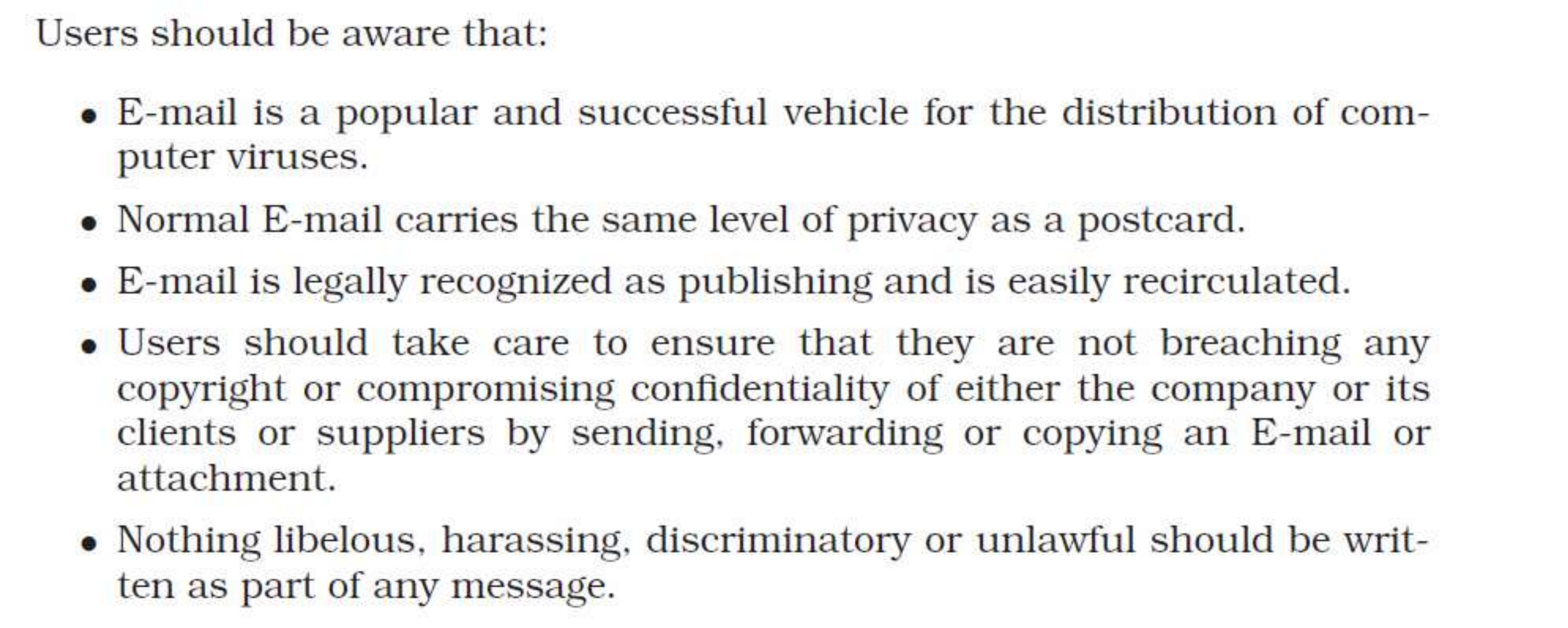
- 5. *Data protection*
- Any person using a computer may be a *data processor*. Every individual is responsible for maintaining confidentiality of data by preventing unauthorized disclosure.6



The act lays out the following principles of data protection:

- Personal data shall be processed fairly and lawfully and such processing must comply with at least one of a set of specified conditions.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- *6. E-mail and SMS*



Users should be aware that:

- E-mail is a popular and successful vehicle for the distribution of computer viruses.
- Normal E-mail carries the same level of privacy as a postcard.
- E-mail is legally recognized as publishing and is easily recirculated.
- Users should take care to ensure that they are not breaching any copyright or compromising confidentiality of either the company or its clients or suppliers by sending, forwarding or copying an E-mail or attachment.
- Nothing libelous, harassing, discriminatory or unlawful should be written as part of any message.

- 7. *The World Wide Web*
- 8. *Transactions*
- 9. *Hardware and software*
- 10. *Surveillance*
- 11. *Usage*
- 12. *Management*

# 5.10.2 Example IT procedure following a breach of policy

- IT policy ought to contain instructions as to how users will be dealt with when they breach policy. There are many ways of dealing with users, with varying degrees of tolerance: reprimand, dismissal, loss of privilege etc.

- Clear guidelines are important for professional conduct, so that all users are treated either equally, or at least predictably.

# 5.10.3 When an employee leaves the company

- A clear procedure is important for both parties:
- • To protect an organization from a disgruntled employee’s actions.
- • To protect the former employee from accusations about what he or she did after their dismissal that they might not be responsible for.
- It is therefore important to have a clear checklist for the sake of security.
- • Change combination locks.
- • Change door keys.
- • Surrender laptops and mobile devices.
- • Remove all authentication privileges.
- • Remove all pending jobs in at or cron that could be logic bombs.

# END