INFORMATION SECURITY

User Awareness and Practices

By
Janet M.
ICT CENTRE
April 2016

Outline

* Information security
* Electronic records management
* UoN authentication systems
* Keeping your computer, applications and data secure
* Online security and privacy
* Password rules

What is information security?

Information security may be defined as the preservation of:

Confidentiality: protecting information from unauthorized access and disclosure;

Integrity: safeguarding the authenticity, accuracy and completeness of information and processing methods;

Availability: ensuring that information and associated services are available to authorized users when required.

Appropriate protection is required for all forms of information, paper or electronic, to ensure business continuity and efficiency, and to avoid breaches of statutory, regulatory or contractual obligations.

Why do I need to learn about information security?

* Isn't that an ICT problem?

Everyone who uses a computer needs to understand how to keep his or her computer and data secure.

Security is everyone's responsibility.

Why do I need to learn about information security?

Organizations and their information systems face security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, theft, fire or flood. Damage caused by breaches such as computer viruses and computer hacking is becoming increasingly common and sophisticated.

Dependence on information systems and services means that organizations are increasingly exposed and vulnerable to security threats; security issues were not always the primary consideration in system design.

What does information security have to do with managing records?

If you are managing your records properly, you should be keeping them secure. This process involves an assessment of how secure it needs to be, depending on the nature, content and importance of it.

Information that will need to be kept secure includes:

- ✓ Personal information. For example student and staff information.
- ✓ Information relating to teaching and research, particularly prior to publication
- ✓ Information relating to the School's/College's/University's commercial interests

As a general rule, if the loss or unauthorized access or editing of the information could cause damage to the School/College/University or stop you from doing your work, it will need greater security.

Consequences of security violations

- Embarrassment to yourself and/or the University
- Having to recreate lost data
- Identity theft
- Data corruption or destruction
- Loss of employee, and public trust
- Costly reporting requirements and penalties
- Disciplinary action (up to expulsion or termination)

Importance of Electronic Records Management

Electronic records management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of electronic records, including the processes for capturing and maintaining evidence of and information for legal, fiscal, administrative, and other business purposes.
The importance of electronic records management is as follows:

- It helps in the investigation and prosecution of e-mail crimes.
- It acts as a deterrent for abusive and indecent materials in e-mail messages.
- It helps in nonrepudiation of electronic communication so that someone cannot deny being the source of a particular communication.

Protecting records in offices and storage areas

Follow these basic security measures to safeguard **physical (i.e., paper) documents** and records:

1. Fit doors and windows in all offices and records storage areas with strong locks.
2. Keep filing cabinets and other records storage areas locked at all times when not in use.
3. Label all files, folders, and boxes so that their contents, dates, and extent are clear.
4. Equip offices and storage areas with fire and security alarms and test alarms regularly.
5. Only permit access to records storage areas to a small number of qualified personnel.
6. Supervise all external visitors whenever they are in offices or records storage areas.
7. Conduct regular security and facility inspections for all work spaces or records storage areas.
8. Destroy obsolete and superseded records securely as soon as they are no longer needed.
9. Maintain full documentation about all records destroyed or transferred.

Protecting electronic records

Follow these steps to safeguard electronic documents and records, including emails:

1. Do not use computer hard drives (C: drives) to store sensitive information. Instead, store sensitive information in formally established electronic record-keeping systems or, in the absence of such systems, in secured network drives.

2. Regularly clean up computers and network locations by destroying superseded or obsolete records that have met their retention periods.

3. Recognize that deleting electronic records is not the same as destroying them. Work with the IT specialists and the records specialists to guarantee that computer systems are configured to ensure that deleted records are permanently removed from network drives or other storage locations.

4. Contact ICT for guidance about ensuring your computer systems are configured with appropriate security systems, anti-virus software, password protection, and automatic time out/lock features to restrict access to password holders only.

5. Contact Records office for guidance about how to create, store, and manage electronic records so that they are safe, accessible, and authentic, now and in the future.

Selecting electronic records storage media & Maintenance

Avoid the use of floppy disks or other forms of magnetic media not specifically designed for purposes of long term storage for the exclusive long-term storage of permanent or unscheduled electronic records.

Ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the current hardware and software. Before conversion to a different medium, you must determine that the authorized disposition of the electronic records can be implemented after conversion;

Prohibit smoking and eating in all areas that contain permanent or unscheduled records;

Back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records should be maintained in storage areas separate from the location of the records that have been copied;

Electronic records storage media

- ✓ External Hard disks
- ✓ Online storage media – Dropbox, google-drive
- ✓ Shared folder - Shared Folders enables you to create file shares and set permissions, as well as view and manage open files and users connected to file shares on the computer. ICT will be making available soon to each member of staff a shared folder facility with 2GB storage capacity on the corporate storage solution.

Preserving Email message records

(a) The names of the sender and addressee(s), including addressees who are cc'd to an electronic mail message;
(b) The date the message was sent;
(c) Message metadata;
(d) Any attachment to the electronic mail message must be preserved in order for the context of the message to be understood; and
(e) Any other transmission data that is necessary for the purpose of providing the context of the record.

NOTE: If an electronic mail system identifies users by codes or nicknames, or identifies addressees only by the name of a distribution list, names on directories or distributions lists should be retained to ensure accurate identification of the sender and addressee(s) of messages that are records.

Provide instructions to electronic mail message users specifying when to request receipts or acknowledgments that indicate that a message has reached a recipient's mailbox that it has been opened for recordkeeping purposes and how to preserve them in electronic mail systems that support such functionality.

Preserving Desktop Documents

Ensure that word-processing, spreadsheet, presentation, task list, contact, calendar and other desktop documents are identified, preserved and disposed of in a manner consistent

Identify and capture desktop documents created and received by employees in remote locations or on external devices, such as in the field or employee home offices, portable devices, such as tablets, notebooks, laptops, personal digital assistants and portable storage devices.

UoN Authentication Systems

Active Directory And Radius (Email and Wi-Fi accounts)

Active Directory

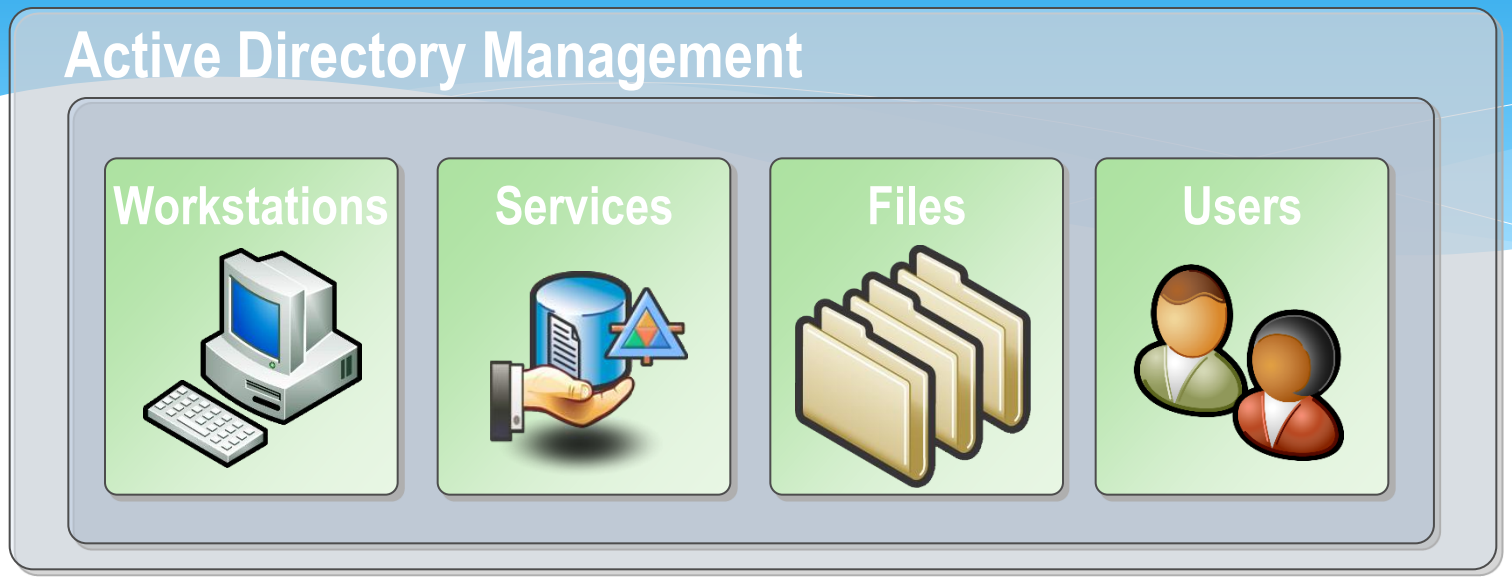
A directory service (DS) is a software application- or a set of applications - that stores and organizes information about a computer network's users and network resources.

Allows network administrators to manage users' access to the resources

Act as an abstraction layer between users and shared resources

- ✓ A single sign-on environment
- ✓ Improved desktop security
- ✓ Improved management and administration of workstations
- ✓ Improved timeframe for updates, patches and installation of new versions of software

UoN Authentication Systems



Format of UoN AD Credentials –

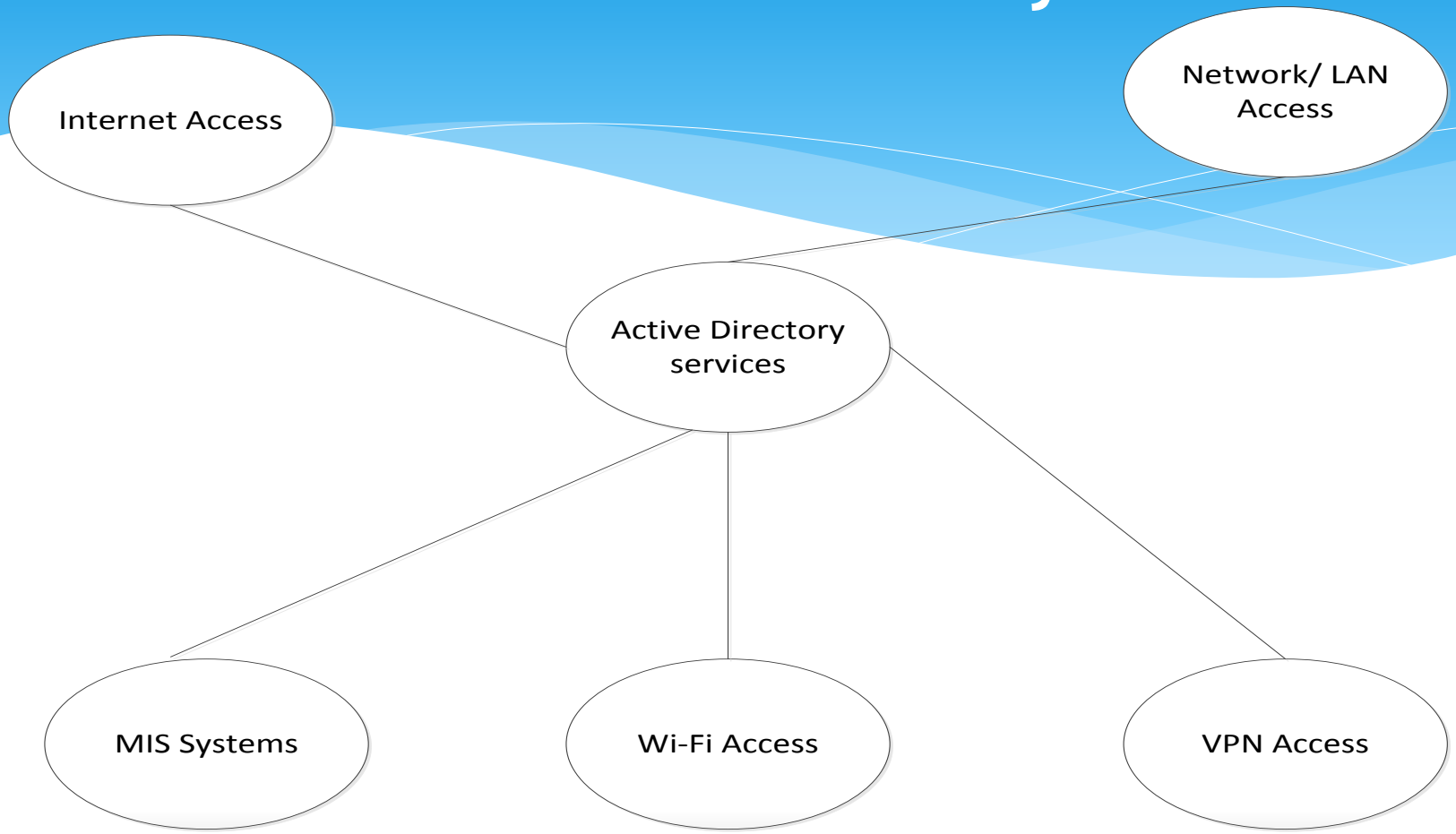
username is user's Payroll number i.e. **216410**, default password is **nairobi123** after which a user can change to a proffered password.

Note: Password expire every 6 months

Further Integration

- Consequently AD will allow ICT to consolidate a number of services and functions onto one platform.
- It will also allow ICT Center to provide critical services and work toward single-sign on for many of the university's support systems.

UoN Authentication Systems



Note: For you to enjoy this benefits, your UoN computer must join Active Directory.

UoN Authentication Systems

Radius

A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

Often used to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server.

In UoN, you will the same username and password to access email, VPN, intranet.

Keeping your computer, applications and data secure

* Use security software e.g Windows Defender, Microsoft Security Essentials, Antivirus. Make sure to have only one antivirus program installed.

* Practice the principle of least privilege (PoLP) - Do not log into a computer with administrator rights unless you must do so to perform specific tasks.

* Maintain current software and updates - Keep your software updated by applying the latest service packs and patches.

* Frequently back up important documents and files - Back up your data frequently. This protects your data in the event of an operating system crash, hardware failure, or virus attack.

Keeping your computer, applications and data secure

* Use security software e.g Windows Defender, Microsoft Security Essentials, Antivirus. Make sure to have only one antivirus program installed.

* Practice the principle of least privilege (PoLP) - Do not log into a computer with administrator rights unless you must do so to perform specific tasks.

* Maintain current software and updates - Keep your software updated by applying the latest service packs and patches.

* Frequently back up important documents and files - Back up your data frequently. This protects your data in the event of an operating system crash, hardware failure, or virus attack.

Avoid threats to your computer

* Never share passwords -Pick strong passwords and keep them private.
* Do not click random links - Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it; delete it.
* Beware of email or attachments from unknown people, or with a strange subject line

* Do not download unfamiliar software off the Internet - Some programs appear to have useful and legitimate functions. However, most of this software is (or contains) spyware, which will damage your operating system installation, waste resources, generate pop-up ads, and report your personal information back to the company that provides the software
* Remove unnecessary programs or services from your computer- Uninstall any software and services you do not need.
* Log out of or lock your computer when stepping away, even for a moment - Forgetting to log out poses a security risk with any computer that is accessible to other people (including computers in public facilities, offices, and shared housing), because it leaves your account open to abuse.

Online security and privacy (Facebook, Twitter, Gmail)

* **Protect Your Accounts with 2 Factor Authentication -** Two factor authentication on websites is an easy and effective way to secure your online accounts.
* **Don't fill out your social media profile.** - The more information you share online, the easier it's going to be for someone to get their hands on it. Don't cooperate.
* **Minimize Access to Your Information** - Limit the audience of your posts and don't share everything. As a general rule, refrain from posting things online that you will regret later.
* **Control What You Can** - Since Facebook is a social networking site designed for sharing information, many of the settings are open by default. It is up to you to access the Privacy Settings and configure the options as you see fit.

* **Beware Friends seeking Money** - Most people know enough to not respond to e-mail requests from exiled Nigerian royalty promising millions of dollars if only you will help them smuggle the money out of the country. Anybody who doesn't know better probably shouldn't be on the Internet; such people are a danger to themselves and others.
* But what if your good friend from high school whom you haven't seen in 18 years sends you a message on Facebook explaining how their wallet was stolen and their car broke down, and asks you to wire money to help them get home? You might not be as apprehensive--but you should be.

* **Apps** - Be careful about using Facebook Apps. Some of the apps can access lots of your personal information and sell your personal information to other parties.
* Do not share any sensitive and private information on wall postings, messages, or feeds. This goes double for any information about your location and whereabouts.
* **Tiny URLs -** Another threat that has emerged as a result of social networking is the tiny-URL attack. Some URLs are very long and don't work well in e-mail or in blog posts, which created a need for URL-shortening services. Twitter, with its 140-character limit, has made the use of URL-shortening services like Bit.ly a necessity.

  Use discretion when clicking/ opening tiny URLs.

Password Rules

* Rule 1 – Password Length: Stick with passwords that are at least 8 characters in length. The more character in the passwords is better, as the time taken to crack the password by an attacker will be longer. 10 characters or longer are better.

* Rule 2 – Password Complexity: Should contain at least one character from each of the following group. At least 4 characters in your passwords should be each one of the following.

* Lower case alphabets
* Upper case alphabets
* Numbers
* Special Characters

Guidelines for avoiding weak passwords

* Password same as username or part of the username
* Name of family members, friends or pets.
* Personal information about yourself or family members. This includes the generic information that can be obtained about you very easily, such as birth date, phone number, vehicle license plate number, street name, apartment/house number etc.
* Sequences. i.e consecutive alphabets, numbers or keys on the keyboard. for e.g. abcde, 12345, qwert.
* Dictionary words. Dictionary words with number or character in front or back
* Real word from any language
* Word found in dictionary with number substitution for word look alike. for e.g. Replacing the letter O with number 0. i.e password.
* Any of the above in reverse sequence
* Any of the above with a number in front or back.
* Empty password

ICT Policy

The UoN ICT policy covers the following:

- ✓ Network Development and Management Policy
- ✓ ICT Security and Internet Policy
- ✓ Software Development, Support and Use policy
- ✓ User Support Services Policy
- ✓ ICT Equipment Maintenance Policy
- ✓ ICT Training Policy
- ✓ Database Administration Policy
- ✓ System Administration Policy
- ✓ Telecommunications Policy
- ✓ ICT Procurement Policy

UoN's WIKI

Site provides information about the UoN Communication and Network Services

Configuration info:

- ✓ Chemichemi
- ✓ Chemiweb
- ✓ Laptop Wi-Fi configurations
- ✓ Network access account
- ✓ VPN
- ✓ Active Directory
- ✓ Corporate Antivirus
- ✓ Basic Troubleshooting

THE END