UoN Workshop on Sensitization on Strategies to Fight Corruption

Presentation on Integrity Program in relation to ICT

June 9th, 2011

Elijah Tenai, Deputy Director(NIS) ICT

tenai@uonbi.ac.ke

The Agenda

1.Who we are

2.Our Mandate

3.Threats to Mandate

4. Role of Computerization to Corruption Prevention

5. ICTC In Corruption Prevention (CP)

6. Your role in Corruption Prevention With ICT

7.Your role in Protection Against Threats

8.Conclusion

Who We Are: Vision and Mission

Our Vision

To be a state-of-the art ICT function powering the university into world-class scholarly excellence

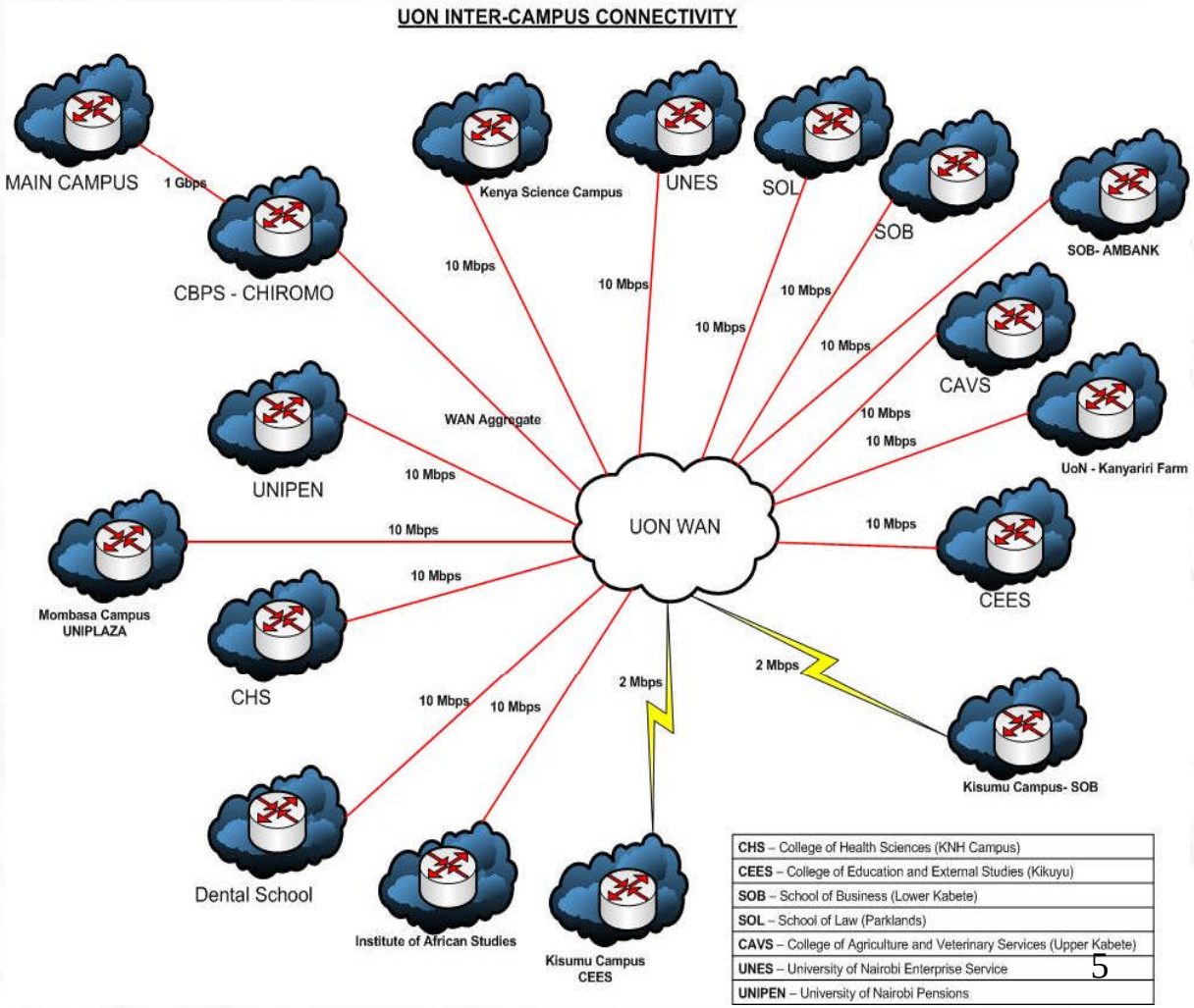
Our Mission

To develop, deploy and support innovative, quality and sustainable ICT solutions and services that meet the changing learning, teaching, research, and management needs of the University

Our Mandate –Computerisation

- Student Management information system (SMIS)
- Room allocation Information System (HAMIS)
- Human Resource Information System (HRMIS)
- The Payroll System
- ACCPAC Financial Management IS (FIMS)
- Budgetary Control IS
- Online Leave Application System (OLAPIS)
- Learning Management Information System (Wedusoft)
- ……

Our Mandate –Network Infrastructure Development and Support



Our Mandate –User Support

Our Mandate - ICT Training

Our Mandate

- Development and maintenance of MIS applications
- Development and support of E-Learning Systems
- Network Management and Communication Services
- User Support Services
- Hardware Maintenance
- ICT Security
- E-mail and Internet access
- Training
- ICT Consultancy

Threats to Mandate - (Some)

- Acts of vandalism, theft
- Viruses and Malware
- Physical Disasters
- Bad User Habits/Social Eng problems
  - -Harambee accounts
  - -Web surfing habits
  - - Physical access control to offices (not strict)
- Aging equipment and Old software
- Computer crime – hackers, phishers
- Unstable/Unclean power
- Low IT literacy
  - choice of/regular change of passwords, deleting infected mails, updating AV, regular scanning of PCs/Removable media
- Quacks/incompetence

Threats to Mandate – (Some) Mitigation

- Virtual LANs (VLANs) organizes network devices into logical workgroups (or broadcast domains) independent of physical location
- DHCP –System that sets network configurations automatically for Computers on the networks
- Network and perimeter firewalls
- Grilles and reinforcement - Computer rooms and labs –security
- Special built Server room
- Web filtering
- Antivirus and Anti-spam solutions
- UPS and Power back-up generators
- User training
- Quacks? - Our ICT officers are available to give necessary support –call upon them

Role of Computerization to Corruption Prevention

- "Temptation for corruption occur where staff have access to a valued resource and to those who will pay for it; and where they have the skills, confidence and autonomy to make decisions about the provision of that resource"

"Corruption is Authority plus Monopoly minus Transparency"

- Computerisation can help restrict/control access to the resource or to the relevant decision-making processes e.g automating certain processes, removing the avenue to corruption

- But there must be a deliberate and systematic design for the specific function – to detect and/or seal a corruption loop-hole.

- "Managers, and officers guarding against corruption, must have the skills, motivation, authority and means to detect and act against corrupt activities, knowing too well it can also be carried out with computerised system."

Role of Computerization to Corruption Prevention - Paradoxes and Myths

- Confidence: Promotes mythical view that computers are all seeing and all knowing, causes some corrupt staff to refrain. What about knowledgeable ICT staff?

- Access: Closes access to some corrupt staff, eg by automating room allocation/fee collection. But, how about the system operators themselves? and hackers in a networked environment?

- Control: Masked with sense of computer omnipotence, some managers make false assumptions that the systems can operate without need for human intervention; wrong, as there is still need to institute controls on computerised systems too

- Skills: 'up-skilling' of corruption-possible. New opportunity for those with ICT skills while suppression on those without

ICTC In Corruption Prevention (CP) – Infrastructure

- The university relies heavily on the ICTC infrastructure to discharge its mandate, helping prevent multitude of possible malpractices.

- Any breakdown can create ripe situations for corruption. Example, a revert to manual processes during room allocation can be exploited to allow corrupt practices such as favoritism or bribery to gain room allocations, and possible revenue loss through incomplete/falsified returns on room occupancy

- ICTC is on continuous improvement of the overall infrastructure, e.g.

1)Upgrading of the Intranet server farm, at cost of approx. Kshs. 50 M.
2) Increasing access to IS using Wi-Fi LANs (Hot Spots). SWA HQ and MC are done. SOB and CBPS, are currently under implementation, CEES, CHS, CAVS, KSC and SOL planned for next year.
3) Campus LAN extensions and upgrades. CAVS campus LAN recently completed at cost of Kshs. 20 M
4)Clean power provision by procuring UPS systems (Aprox. Kshs. 5M)
5) Extension of UoN WAN to cover extra-mural centers (Kakamega, Nakuru, Meru, Garissa etc) ongoing

…

ICTC In Corruption Prevention (CP) - MIS

ICTC develops and facilitates running of various systems and computerization processes with immense benefits to CP:

1. Human Resource Management system (Kshs. 15) - Improved payroll processing with no delays in payment; Online leave application

2. Student Management Information System (Kshs. 25M) - Improved revenue collection; Improved service delivery; Reduction in turn-around time for processing transcripts

3. Student Clearance System (Kshs. 2M) - Eliminate Favoritism in clearance process; Reduce time wastage as students need not be present at point of clearance

4. ACCPAC financial system (Kshs. 18M)– Improved turnaround time for financial reporting; Eliminate pilferage of revenue

…

ICTC In Corruption Prevention (CP) – Information Dissemination

ICT runs forums for disseminating and encouraging compliance to various policies and guidelines, including information to guide responsible use of the computer systems and on CP.

1. Integration of basic security awareness training in the regular MIS system users training such as how to ensure strong passwords and care in sharing confidential information through phones

2. Online postings of usage policy for the various ICTC systems, eg the WiFi usage policy under wiki.uonbi.ac.ke, the ICTC policy and various UoN policies under intranet.uonbi.ac.ke

3. E-mail alerts on possible suspected security threats and ways to protect

ICTC In Corruption Prevention (CP) – System Audit Trails

A database audit trail mechanism has been integrated to track activities on critical MIS systems such as records entry, updates, or deletions, to facilitate detection of unauthorized manipulation of data.

The trails are accessible only to select senior staff who are responsible for enforcement of system data integrity.

ICTC In Corruption Prevention (CP) – Policy Enforcement

Example: Password Policy. ICTC has been improving the systems of password management across the the range of systems of the University, including the following steps taken in the recent past:

1) Enforcement of requirements for mandatory passwords changes after every 3 months for users of E-mail and some MIS systems. - Reduces the window of exposure to the risk through compromised passwords. Also help in automatically disabling dormant accounts

2) For some critical systems activities such as updates on Students Management Information Systems, other than passwords access control, the services are tied to specific computer consoles using their unique hardware addresses. Shrinks the risk exposure to fewer machines, whose owners are known

Your role in Corruption Prevention With ICT

- Familiarize yourself with the policies, standards, and regulations
  - Visit Intranet.uonbi.ac.ke
- Make personal efforts and encourage corporate initiatives to proper values and ethics, honesty and integrity. Be familiar and subscribe with National and International Benchmarks and values demands
  - –The Public Officer Ethics Act 2003
  - –The new constitution
- Adopt ICT as a lifestyle
  - -Sense of ownership of ICT service/solutions/processes in place at UoN
  - -Participation in conceptualization, development, and operations
  - - Feedback for improvement
  - - Use shared resources diligently eg Bandwidth, storage space
  - -Appreciation and Support
- CP is ultimately shaped by mngt decisions and by broader organizational culture than by ICT tools alone; hence all must play their role.
- As a mngr, enforce checks and balances both before and after computerization

Your role in protection against threats

- Never dis-close or share your password under any circumstances!
- Change your Password regularly . Use strong passwords. Do not recycle old passwords
- Minimise use of removable media eg flash disks –insist on email if not sure
- Ask for help from ICT Staff

•----------Original Message ----------

•Subject: Email Administrative Notice.

•From: "University of Nairobi E-mail CustomerCareDepartment."

•<jimlai@netvigator.com>

•Date: Fri, May 13, 2011 9:39 am

To: undisclosed-recipients:;

Attention: University of Nairobi Email User,

You have exceeded your University of Nairobi e-mail account limit quota of 150MB and you are required to expand it within 48 hours or else your University of Nairobi e-mail account will be disable from our database.

In order to expand your University of Nairobi e-mail account quota to 250GB, we require your E-MAIL username and Password. Please urgently send these details as soon as possible.

•Thank you for using our email services.

•Copyright Â©2011 University of Nairobi E-mail CustomerCare

Your role in protection against threats

- Beware of the dangers of experimenting! >>>>
- Keep your desktop firewall turned on always
- Ensure you have upto date Antivirus software
- Turn-off your Computer when not in use
- Don't forget physical security!

Sometime the damage is done without intent (passive hacking)

–People making mistakes:

*delete –rf** at root directory

Only give superuser/server access privileges to people who know what they are doing!

–People prone to tantalizing messages

“LIVE-Double click on attached video to watch Lewinsky and Clinton …”

“You've Won $1,000,0000 Lottery”

–People experimenting with things they’ve heard about

“I was just testing this downloaded script....”

Be Careful What You Download!

Conclusion

ICTC systems and tools at the University are continually being shaped to play their potential role in CP and Integrity Assurance.

This role is however limited, it is part of a much larger jigsaw, for which you as a stakeholder have an inevitable part to play.

Thanks for your time!