

CODE OF PROFESSIONAL PRACTICE

**PAPER PRESENTED AT 2009 ANNUAL INDUCTION CEREMONY
OF COMPUTER PROFESSIONAL REGISTRATION COUNCIL OF
NIGERIA**

BY

OJINTA K. OJI-ALALA, *FNCS*

JUNE 25, 2009

INFORMATION TECHNOLOGY CODE OF PROFESSIONAL PRACTICE

1.0 The Computer Professionals (*Registration Council of Nigeria*) sets and enforces the standards of competence, conduct and ethical practice for the Information Technology Profession in the Federal Republic of Nigeria. To achieve this objective the Council has established a set of standards of technical capability (knowledge and skills) which members must satisfy, and a set of standards of conduct to which members must conform. The Code of Ethics and Professional Conduct for Information Technology Professionals was adopted by the members of the Profession at the 7th Annual General Meeting on September 27 2001.

This presentation recognizes that inductees and others have gone through series of training and orientation in computing and the use of computational machinery that should qualify them to be Information Technology Professionals. The law establishing Information Technology as a profession stipulates that for anyone to practise in Nigeria, he/she must be a registered member of the profession. Therefore, he/she has to abide by the rules and regulations of the profession and adhere to the necessary obligations to the profession and society in which we operate.

1. **RESPONSIBILITY OF COUNCIL**

it is the responsibility of Council to control and supervise the Information Technology Profession in Nigeria. According to the law, the profession is that of using computational machinery and other related techniques. The general characteristics common to most professions will be discussed after in this presentation.

2. DUTY OF COUNCIL

- Determine what standards of knowledge and skills are to be attained by persons seeking to become members of the Profession and improving those standards from time to time as circumstances may permit.
- Secure, in accordance with provisions of this Act, the establishment and maintenance of a register of persons seeking to be registered under this Act to practice the profession and the publication, from time to time, of the list of those persons.
- Perform through the council, the functions conferred on it by the Act. According to section 14(6) of the Act, the “council may make rules not inconsistent with the Act is to acts which constitute professional misconduct”.

1.1 CODE OF ETHICS & CODE OF PROFESSIONAL PRACTICE

These codes are the set of rules that govern the behaviour and responsibilities of members. According to the British Computer Society Handbook 6:

The code of practice deals with the ways in which all registered members are expected to exercise their professional competence and thereby complement its companion, the code of conduct (Ethics) which deals with behaviour.

The two codes apply to all members of the profession. . Considering that we are operating at these times when Information Technology is affecting the commercial and social life of people and the way we are governed, it is important for the profession to not only state clearly its rules, but to ensure their adherence.

In summary, while the **Code of Ethics** is concerned with the character and behaviour of members of the profession, the **Code of Professional Practice** is concerned with professional responsibilities, consisting essentially of statements which prescribe minimum standards of practice to be observed by all registered members.

The Australian Computer Society, handbook states as follows:

The Code of Professional Conduct is aimed specifically at the individual IT professional and is intended as a guideline to acceptable personal conduct for each IT professional practicing in the industry. It is applicable to all IT professionals regardless of their role or specific area of expertise.

The Code of Professional Practice is intended as a guideline for acceptable methods of practice within the IT industry. Because of the rapid changing nature of the IT industry and the wide variation in roles, this section of the code is deliberately generic and concentrates on common areas encountered the industry that are not influenced by hardware, software or organization type .

Under the Code of Ethics, the following obligations have been established by council and we shall not get into details as they have been discussed in a different session.

- To the public (safety, health and well-being)
- To employer or client (trust, faithful service, advice, guidance of interest, honesty)
- To fellow members of the profession (cooperation, honesty and respect)
- To the profession (competence, promotion, enhance prestige)
- To my country (respect & honour, law abiding, transparently honest, integrity, responsibility and reliability)

It is important to stress that IT professionals must not engage in any conduct or commit any act which is discreditable to the reputation or integrity of the profession.

1.2 ETHICAL CODES COMMON TO IT PROFESSIONAL BODIES

The following four IT bodies met to compare notes on ethics and virtually agreed on major issues as stated below.

- Association for Computing Machinery (ACM) – Computer scientists.
- Institute of Electrical and Electronics Engineers – Computer Engineers
- Data Processing Manager Association (DPMA) – Managers of Computer Systems & Projects
- Institute for Certification of Computer Professionals (ICCP) – Voluntary Certification Mechanism for Computer Professionals.

1. *Personal Integrity/Claim of Competence*
2. *Personal Responsibility for work*
3. *Responsibility to Employer/Client*
4. *Responsibility to Profession*
5. *Confidentiality of Information*
6. *Conflict of Interest*
7. *Dignity/Worth of People*
8. *Public, Safety, Health & Welfare*
9. *Participation in Professional Societies*
10. *Increase Public Knowledge about Technology*

With the exception of the concern raised about privacy and confidentiality of data, the codes could have been written to cover most professions. Larry

Colero, Crossroads Programs Inc. opined that the principles of Professional Ethics(required behavior), within the context of professional practice such as law, medicine, accounting, or engineering, include:

Impartiality and Objectivity

- Openness; full disclosure
- Confidentiality
- Due diligence/duty of care
- Fidelity to professional responsibilities
- Avoiding potential or apparent conflict of interest.

Principle of Global Ethics

- Global justice (as reflected in international law)
- Society before self/social responsibility
- Environmental stewardship
- Interdependence & responsibility for the whole
- Reverence for place (serves to test for shyness since it is not an obvious one).

An added measure of accountability is placed on globally influential enterprises such as government and transnational corporations.

2.0 CODE OF PROFESSIONAL PRACTICE

2.1 Practices common to all disciplines: Each of the undermentioned principles is fundamental to good professional practice, and they are not in any order of importance.

- Service to the public
- Responsiveness to the government and the needs of the public
- Accountability
- Fairness and Integrity
- Efficiency and effectiveness

These ethical principles help us decide whether our actions are right or wrong. It will be advisable that IT professionals should ask themselves these questions:

- Are my actions within the spirit and letter of the law?
- Are my actions consistent with the organization's goals, the values and principles of the code of Ethics and Professional Practice?
- Could I adequately defend my action to my boss or chief executive and the community if the situation became publicly known?
- Is this the proper thing for me to do?
- What will the outcome of my action be for:
 - The organization, the department and the public interest
 - Staff
 - Clients/Customers
 - My colleagues
 - Other
 - Me?

IT professionals should act within the spirit of the law and the code. It is not sufficient to think that your behaviour is ethical, it must also be seen to be so.

2.2 WHO MUST COMPLY WITH THE CODE?

The code applies to and binds all members of the IT profession.

2.3 WHEN DOES THE CODE APPLY?

The obligations of the code apply at all times, including when the IT practitioner is not in his/her place of work or performing the work duties. It includes time when the IT professional is on vacation.

2.4 WHAT HAPPENS IF ONE BREACHES THE CODE?

Information Technology Professionals hold special positions of trust, especially regarding young people in our communities, and must be accountable for their actions at all times.

When it is considered that the code has been breached, disciplinary action may be taken. Any disciplinary action shall be taken in accordance with the principles of natural justice and procedural fairness in a manner that promotes the values and general principles of Act 93 of 1993.

In deciding whether the code has been breached, due consideration will be given to the circumstances of the breach and the views of the IT professional concerned.

The primary aim of disciplinary action is to maintain proper standards of conduct by IT professionals, to protect the reputation of the council and the registered members, and to maintain public confidence in the integrity of the council. The aim is not to punish, even if the consequences of disciplinary action are severe. Disciplinary action is as stated in the law establishing the council and may include:

- Counseling
- A written admonition
- A financial penalty
- Removal from the register

Or as may be determined by a Tribunal or High Court of Nigeria.

2.5 WHO DETERMINES IF THE CODE HAS BEEN BREACHED?

The computer Professionals Registration Council makes a decision whether the code has been breached and what disciplinary action should be taken.

The process of going through the Investigating Panel and the Disciplinary Committee when a case is reported is stated in the Act.

2.6 UPDATING THE CODE

The code is updated from time to time by the council in order to take care of new concerns about ethical issues for it to be current and relevant.

2.7 CODE BODY OF KNOWLEDGE

In Australia, Nov 1992, the Australian Computer Society published a report entitled : "The ACS Towards 2000." One of the terms of reference emerging for the study was to "determine the common body of knowledge appropriate to the overall discipline of Information Technology."

The general terms the core body of knowledge as applied to the profession typically include:

CORE BODY OF KNOWLEDGE

- The 'Core' (a standard educational curriculum)
- A requirement to hold an approved tertiary qualification
- Relevant experience
- A code of Ethics
- Acceptance of personal liability
- A commitment to continuing professional development
- A license or certificate to practice.

AREAS OF KNOWLEDGE

1. Computer Organization & Architecture
2. Conceptual Modeling

3. Database Management
4. Data Structures and Algorithms
5. Data Communications & Networks
6. Discrete Mathematics
7. Ethics/Social Implications/Professional Practice
8. Interpersonal Communications
9. Program Design & Implementation
10. Project Management & Quality Assurance
11. Security
12. Software Engineering & Methodologies
13. Systems Analysis & Design
14. Systems Software

3.0 PRACTICES COMMON TO ALL DISCIPLINES

3.1 CODE OF PROFESSIONAL PRACTICE (Australian example)

This is designed to provide members with authoritative guidance on acceptable standards of professional conduct and practice within the IT industry.

1. **The Public Interest:** Safeguard the interests of your clients provided that they do not conflict with the duties and loyalties owed to the community, its laws and social and political institutions.
2. **Integrity:** Do not breach public trust in the profession or the specific trust of your clients and employers.
3. **Confidentiality:** You must not disclose information acquired in the course of your professional work except where consent has been

obtained from the rightful legal owner or where there is a legal or professional duty to disclose.

4. **Objectivity and Independence:** Be objective, impartial and free of conflict of interest in the performance of your professional duties.
5. **Competence:** Accept only such work as you believe you are competent to perform and do not hesitate to obtain additional expertise from appropriately qualified individuals where advisable.
6. **Subordinates:** Ensure subordinates are trained in order to be effective in their duties and to qualify for increased responsibilities.
7. **Responsibility to your Client:** Actively seek opportunities for increasing efficiency and effectiveness to the benefit of the user.
8. **Promoting Information Technology:** Endeavor to extend public knowledge, understanding and appreciation of Information Technology.
9. **The Image of the Profession and the Society:** Refrain from any conduct or action in your professional role which may tarnish the image of the Information Technology Profession or unjustly detract from the good name of your professional body.

4.0 **KEY INFORMATION TECHNOLOGY PRACTICES**

Under this broad outline, we would briefly discuss the following major practices:

- Project Management
- Relationship Management
- Security
- Safety Engineering
- Change Management
- Quality Management

4.1.0. **PROJECT MANAGEMENT**

Project management is the discipline of planning, organizing and management of resources, to bring about the successful completion of specific project goals and objectives. The primary challenge of project management is to achieve all of the project goals and objectives while honoring the preconceived project constraints like scope, time and budget.

4.1.2 **WHEN DEFINING A NEW PROJECT**

- Encourage your customer to:
 - Explain fully the corporate objectives that underpin the requirements, the scope, issues, constraints and risks to be addressed.
 - Articulate clearly the desired business benefits and how they will be measured.
 - Explain fully the project derivables.

- Define the information and services that your customer will provide.
- Select and list appropriate quality standards and procedures.
- Devise an acceptable strategy that will fairly demonstrate that the requirements of the project have been met.
- List your assumptions, especially those that relate to goods or services provided by your customer, and gain your customer's approval of their validity.
- Define the escalation/exception procedures to be followed in the event of deviation from the plan.

4.1.3 **WHEN PLANNING**

- Ensure that the scope, deliverables, timescales, costs and responsibilities are agreed in advance.
- Make realistic estimates of the costs, timescales and resource requirements.
- Resists the pressure to accept estimates produced in earlier stages.
- Beware of the pitfalls associated with estimating tools; use other methods to double-check the feasibility of the results.
- Assure yourself that you have the resources required to complete the project within the agreed costs and timescales.
- Do not depend on later contract changes to recover overspend.

4.1.4 **WHEN MANAGING PROJECT RISK**

- Seek out the real risks to customer, the organization and any suppliers.
- Openly discuss with the customer the options for allocating,

managing, mitigating and ensuring against the risks.

- Avoid accepting risk that would be better owned by the customer.
- Devise mitigation actions that will reduce the chances of most services risks happening.
- Make yourself aware of the differences between civil and criminal law in the treatment of risk.

4.1.5 WHEN MANAGING AND DEPLOYING THE PROJECT TEAM

- Ensure that all team members are given written instructions on each task to be performed with target completion dates.
- Monitor the deployment of individuals objectively to ensure that they are contributing effectively while developing skills and experience.

4.1.6 WHEN TRACKING PROGRESS

- Maintain metrics on all project activities, so that later projects can benefit.
- Provide early warning of any possible overrun to budget or timeline, so that appropriate actions can be taken.
- Do not assume that any overruns can be recovered later in the project; in particular do not cut back on later activities such as testing.

4.1.7 WHEN CLOSING A PROJECT

- Honestly summarise the mistakes made, good fortune encountered and lesson learned.
- Recommend changes that will be of benefit to later projects.

4.2.0 RELATIONSHIP MANAGEMENT

Relationship Management in this context will deal with managing customer and supplier relationships.

Customer Relationship Management (CRM) consists of the processes an organization uses to track and recognize its contacts with its current and prospective relationships software based approach handling customer relationship.

4.2.1 WHEN SEEKING NEW CUSTOMERS

- Ensure that a common understanding exists throughout the organization of its corporate objectives, market position, product lines and development plans and that these form the basis of marketing strategy.

4.2.2 WHEN SELLING TO PROSPECTIVE CUSTOMERS

- Do not overstate the capabilities, performance, and benefits of the proposed product or services.
- Make your prospective customer aware of any risks in your proposed solution.
- Identify to your prospective customer any additional costs or changes necessary to make effective use of the proposed products and services.
- Maintain contact with your prospective customer after conclusion of the sales activity; client any shortcomings in the sales activity and initiate remedial action.

4.2.3 **WHEN NEGOTIATING CONTACTS AND SERVICE LEVELS**

- Avoid later disappointment by negotiating achievable service levels at realistic prices.
- Avoid situations that could later be interpreted as corrupt (accepting or giving lavish gifts, entertainment, etc)

4.2.4 **WHEN MANAGING CUSTOMER RELATIONSHIP**

- Instill in your customer, a well-founded confidence in the products and services to be delivered, and your commitment to performance, risk, timescales, and delivery.
- Set targets and monitor performance against these targets, aiming to exceed the contractual targets.
- Keep your customer informed of any problems that might arise on the quality of the deliverables.
- Do not sub-contract out any of your responsibilities without prior agreement by your customer; if you do sub-contract, fulfill your responsibilities for the performance of the work.
- Respond promptly to your customer's queries and complaints and ensure that all necessary actions are taken.
- Ensure that the necessary processes and procedures are in place to maintain or recover the delivery of systems and services in the event of any physical technical or environmental disaster or major outage, providing continuity of service to your customer.

4.2.5 **WHEN MANAGING SUPPLIER RELATIONSHIP**

- Act impartially when selecting new suppliers; establish evaluation

criteria that are not biased towards a particular solution and apply the criteria rigorously to all proposals.

- Encourage resolution of any shortcomings in the service, through proper communication between all parties, rather than resorting to penalty clause.
- Provide regular feedback to the supplier, so that any improvements can be made before any problems become serious.

4.3.0 SECURITY

The object of security management is to eliminate or minimize computer vulnerability due to destruction, modification or disclosure. Security should be administered in the context of how the organization needs to control, use, and protect its information. Protection needs to be appropriate and reasonable given management's risk posture. Three levels of security (physical, procedural, and logical) used in tandem can reduce the risks.

4.3.1 WHEN ASSESSING RISKS

- Resist any pressure to oversimplify the risk analysis; involve personnel at all levels within the organization to elicit the threats and the value abilities to those threats.
- Ensure that the decision-makers are fully aware of all the relevant facts and the possible consequences of their decision.

4.3.2 WHEN IMPLEMENTING COUNTERMEASURES

- Recommend a balanced and cost-effective mix of countermeasures that offer the required levels of confidentiality, integrity and

availability.

- Promote a culture within the organization where everyone recognizes the importance of security and is aware of their responsibilities for potential breaches of security.
- Whilst dealing sensitively with people, be aware that breaches of security are more likely from within the organization.

4.4.0 **SAFETY ENGINEERING**

This has to do with building new systems and assessing complexity. The field of interest is in the theory, design, development and implementation of product safety engineering for electronic and electro-mechanical equipment and services.

4.4.1 **WHEN BUILDING A SYSTEM**

- Examine the proposed use of proprietary digital communication systems and seek out common-cause failures between control and protection function.
- Beware of novel approaches to specification, design and implementation of knowledge-based computing and control systems; be attentive to their attendant problems of verification, and the effect on safety-related operation.
- Determine the adequacy of the protection and control systems for remote plants, enumerate the hazards to which the plant may be subjected and relate each to the proposed protection and control systems.
- Establish that the proposed integration of the mechanical structures (moving parts) with micro-electromechanical (MEMS) components is based on components intended for mechanical operation based on computer control.

- Beware that the overall behaviour of systems based on software and components of unknown or uncertain pedigree (SOUP) and commercial off-the shelf product (COS) will be affected by software components not specifically designed for safety purpose.

4.4.2 **WHEN ASSESSING COMPLEXITY**

- Only use evaluated and validated software languages or accredited components for control systems.
- Establish/Determine practicable software development methods and validation tools for embedded software, particularly in small systems.
- Apply 'proven in use' analysis to achieve the appropriate level of safety integrity for opto-electronic components/techniques used for the sensing of personnel presence.
- Beware that increased complexity of smart sensors increase the possibility of systemic failure; that there is a need for software and firmware version control; that, operationally, there is a dependence on configuration management by the user.

4.5.0 **CHANGE MANAGEMENT**

4.5.1 Change Management is an IT service management discipline that ensures that standardized methods and procedures are used for the efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. This section will deal with business change and when to control changes.

4.5.2 WHEN ADVISING ON BUSINESS CHANGE

- Appreciate the implications of new process on both people and the organization; identify the activities necessary to ensure a smooth transition to the new processes.
- Challenge any apparent malpractices and investigate the root causes.
- Highlight and drawbacks as well as the benefits of proposal changes.
- Show sensitivity to political and cultural issues as well as technical and business effectiveness targets.
- Monitor the progress of the changes, learning from any mistakes made and, where possible, resolving any problem encountered.

4.5.3 WHEN CONTROLLING CHANGES

- Promote the importance of a structured change management process, where all changes are prioritized, assessed and tracked.
- Ensure that the appropriate impact analysis is conducted before any change is authorized.
- Check each change provides a cost-effective solution to a technical and/or business need, and is prioritized accordingly.
- Keep to a minimum the number of changes to be made at a given time.

4.6.0 QUALITY MANAGEMENT

Quality Management is focused not only on product quality but also the means to achieve it. This section will deal on quality system, standards, assurance and audit

4.6.1 WHEN ESTABLISHING A QUALITY SYSTEM

- Express the organization's commitment to quality through a clear and concisely written quality policy.
- Make all members aware of the quality policy.
- Make a clear distinction between mandatory, optional and advisory standards.

4.6.2 WHEN CONSTRUCTING NEW QUALITY STANDARDS

- Involve those who will follow the new standards in the writing and reviewing.
- Keep the language simple; avoid jargon wherever possible.

4.6.3 WHEN MANAGING A QUALITY SYSTEM

- Appropriately recognize individual achievements in attaining quality targets.
- Regularly review the standards and strive for continuous improvements.

4.6.5 WHEN PERFORMING A QUALITY ASSURANCE FUNCTION

- Ensure that every project or product has a quality plan.
- Act as the quality champion in reviews and testing.

4.6.6 WHEN CONDUCTING QUALITY AUDITS

- Create a program for audits to demonstrate that the organization's Quality System is operating effectively and providing management with that sufficient control and visibility.

- Welcome external auditors into the organization.
- Follow up the audits and make sure actions are being taken to make real improvements.

5.0 PRACTICES SPECIFIC TO EDUCATION AND RESEARCH FUNCTIONS

5.1.0 This area will deal with preparation and delivering courses, and assessing and tutoring students.

5.1.1 WHEN PREPARING COURSES

- Ensure the curriculum is founded upon research, practice and/or scholarship.
- Ensure students are equipped with the necessary underpinning to comprehend future developments.
- Expose students within the curriculum to legal, social, cultural and ethical issues.

5.1.2 WHEN DELIVERING COURSES

- Develop in each student an independence of thought and learning ability and thus prepare students for career progression.
- Make explicit to all stakeholders the outcomes to be expected from engaging in the study.

5.1.3 WHEN ASSESSING STUDENT ABILITY

- Ensure that assessment is fair in its discriminatory function.
- Develop yourself as a reflective and reflexive educational practitioner, building on students feedback as appropriate.

5.1.4 WHEN TUTORING STUDENTS

- Encourage students to join a professional body, either now or later, as part of their carrier plan.
- Ensure that students are made aware of the code of Ethics and professional practice and emphasize the importance of adhering to them, whether or not they join a professional body.
- Ensure that students are made aware that their course cannot cover all the technical details of specific topics in computing and that their technical knowledge will need to be constantly refreshed through continuing education provided by NCS/CPN
- Ensure that students recognize the nature and unacceptability of plagiarism.
-

5.2.0 **RESEARCH**

5.2.1 **When Performing Research**

- Pursue research only in those areas that offer benefits to the organization or its customers but not to the detriment of society or the public.
- Avoid providing IT support to research on human subjects and animals where such research is not legal, consensual, or (in humans) authorized by the subject.
- Strive to safeguard the confidentiality and anonymity of private data used in research.
- Where allowed by the organization, share the results of your work with other researchers, through papers issued through research publications and presented to conferences.

6.0 PRACTICES SPECIFIC TO BUSINESS FUNCTIONS

6.1.0 The specific practices to be discussed here include:

- ❖ Requirements Analysis and Specifications
- ❖ Software Development
- ❖ Systems Installation
- ❖ Training
- ❖ System Operations
- ❖ Support and Maintenance

6.1.1 REQUIREMENTS ANALYSIS AND SPECIFICATION

This section will deal with conducting systems and business analysis.

6.1.2 WHEN CONDUCTING SYSTEMS AND BUSINESS ANALYSIS

- Assure yourself of the soundness of your analysis methods; that they will deliver an accurate representation of the requirements, enable a seamless transition into design and provide a sound basis for testing and acceptance.
- Strive to understand the organization's business and search for changes that will bring tangible benefit.
- Involve and consult representative stakeholder group.
- Consider the impact of new systems on the public and avoid solutions that impose unacceptable levels of risk on their mental or physical well-being.
- Demonstrate n understanding of the business issues; be persuasive and explain to users and management. In language they understand,

the benefits of the changes being introduced, as well as identifying any drawbacks and trade-offs.

- Document the result of the analysis in a style that can be understood by the users and the developers.
- Explain your analysis methods to the users and encourage them to understand the results and verify their correctness from new, seek out existing designs that could be re-used.
- Check the products of your designs can be used by both experienced and inexperienced user; in particular check that they can be used for training purposes (e.g. on- line help, training databases).

6.2.0 WHEN CREATING WEB SITES

- ❖ Ensure the organization's practice on the collection and use of personal data comply with application national, regional and international laws and (self) regulatory schemes.
- ❖ Construct a privacy statements that protects the rights of consumers and make this statement visible at the web site.

6.2.1 WHEN PROGRAMMING

- ❖ Strive to produce well-structured code that facilitates testing and maintenance.
- ❖ Produce code that other programmers will find easy to maintain.
- ❖ Wherever possible, avoid platform-specific techniques that will limit the opportunities for subsequent upgrades.
- ❖ Check that the code is in accordance with the design specification and resolve any differences.

6.2.2 WHEN TESTING

- ❖ Plan the tests to cover as many paths through the software as possible, within the constraints of time and effort.

- ❖ Promote the use of test tools that will maximize the effectiveness of the testing.
- ❖ Recommend improvements that will improve the effectiveness of the software under test.
- ❖ Maintain a detailed testing log.
- ❖ Accurately document all anomalies arising during the testing and make sure they are investigated.
- ❖ Design regression testing to identify any undesirable side effects of software change.
- ❖ Resist any pressure to curtail testing; make professional advice formally aware of the consequent risks.

6.2.3 **WHEN WRITING TECHNICAL DOCUMENTATION**

- ❖ Document all work to a level of detail that others could take over your work if need be.
- ❖ Follow the appropriate documentation standards; the organization's honest-style and specific standards for the type of document.
- ❖ Strive to keep document up to date.
- ❖ Ensure documentation is sufficient to enable effective maintenance.

6.2.4 **WHEN WRITING USED DOCUMENTATION**

- ❖ Investigate the subject of the documentation, through hands-on use, talking to experts and reading related documents.
- ❖ Strive to understand the potential readership, their expectations and abilities.
- ❖ Write the document in a straight forward style appropriate to the readership, avoid jargon.
- ❖ Use diagrams that complement the text and aid understanding.
- ❖ Check with experts that the document is correct and with potential readers that it meets their expectations.

6.3.0 **SYSTEM INSTALLATION**

This section deals with the installation of hardware and software, and testing installation.

6.3.1 **WHEN SCHEDULING INSTALLATION WORK**

- Ensure that the Installation procedures identify all relevant safety and security procedures.
- Ensure that appropriate licenses exist for all software to be installed.

6.3.2 **WHEN INSTALLING HARDWARE OR SOFTWARE**

- Reduce the risk of installing faulty items, by checking that all necessary pre-installation tests have been performed on all items to be installed.
- Ensure that up-to-date virus checking is in place to reduce the risk of installing any virus.
- Follow all applicable safety procedures and encourage others to do likewise, even if they are not under your control.
- Wherever practical, involve the future users of the system, so that they understand its architecture and characteristics and will be able to perform well-defined maintenance work on their own.

6.3.3 **WHEN TESTING INSTALLATIONS**

- Do not ignore seemingly trivial faults in order to meet deadlines.
- Record all exception events and ensure actions are taken to investigate them.

6.3.4 **WHEN HANDING OVER THE COMPLETED INSTALLATION**

- Provide documentation of all outstanding problems.

- Ensure that the users are capable of taking over the installation, identifying any additional training that may be necessary.
- Provide contract details so that you can resolve any problems that may arise following hand-over
- Identify business continuity planning requirements and ensure the customer agrees to develop a disaster recovery plan which will maintain the continuity of the system to an appropriate level.

6.4.0 **TRAINING**

This section provides information about producing training plans and course material, as well as assessing the success of a training course.

6.4.1 **WHEN PRODUCING TRAINING PLANS**

- Seek out where the organization could improve through increased training and pursue the necessary budgeting.
- Identify training which can be provided by experts in that particular area, nominate individuals with that expertise and attitude to make good trainers, and arrange any necessary instruction training.
- Arrange for suitably equipped facilities in an environment conducive to training.

6.4.2 **WHEN DESIGNING TRAINING COURSES**

- Take into account the abilities of the trainees, structure the content and duration of the courses to avoid overload through variety and breaks.

6.4.3 **WHEN PRODUCING COURSE TRAINING MATERIALS.**

- Write training manuals that complement existing documentation (e.g. user manuals), reflect the structure of the training courses and provide a useful form of reference following the training courses.
- Construct examples, both compatible with the training manuals and relevant to the business, so that trainees can apply the training to normal working situations.
- Design tests that will enable the trainer to assess trainees abilities objectively.
- Review the training material with the trainers and improve the training material following any wide ranging and detailed questing.

6.4.4 **WHEN DELIVERING A TRAINING COURSE**

- Encourage an atmosphere where trainees feel comfortable about asking questions, either during or at the end of training as appropriate.
- Respond to questions form all trainees, avoid favoritism.
- Monitor the performance of trainees, through questions and exercise, identify where trainees are advancing at different paces and resolve any great discrepancies (e.g. separate into groups)
- When an individual trainee is not keeping up with the rest of the class, avoid personal criticism and discourage ridicule by other trainees; if appropriate removing the trainee form the course.

6.4.5 **WHEN ASSESSING TRAINEE ABILITY**

- Assess objectively, against preset criteria, the mastery of skills by trainees and, in accordance with the organization's policy.
- Ensure that all records of assessment are stored securely and are only accessible by authorized individuals.

- Refrain from citing examples of the performance of particular trainees during future training courses.

6.4.6 **WHEN EVALUATING THE BENEFITS OF TRAINING**

- Record in the course completion form possible improvements to the course and additional training requirements for the training.
- Monitor metrics produced by the organization (production rates, failure rates) and demonstrate where training has improved, or additional training could improve these metrics.
- Periodically review the training plan and implement improvements.

6.5.0 **SYSTEM OPERATION**

This section provides information about performing database administration and managing IT assets.

6.5.1 **WHEN MANAGING SYSTEMS OPERATIONS**

- Ensure that you are up to date with and abide by all applicable health and safety regulations.
- Maintain your awareness of other options for providing IT such as outsourcing, new approaches to recruitment and retention, and global supply contracts.
- Regularly review new developments and price changes (network tariffs, license fees), recommending changes to the organization when they offer both cost-savings and acceptable service levels.
- Use appropriate capacity management tools to monitor the hardware, software and networks to provide early warning or prediction of capacity problems; initiate actions (such as procurement of additional equipment) to prevent capacity.
- Establish a configuration management system that tracks the

delivery and formal testing of configuration items, the content of each build and the status of all defects.

6.5.2. WHEN ASSURING BUSINESS CONTINUITY

- Use business impact analysis methods, tools and techniques as appropriate to identify business processes critical to the continuity of the organization.
- Define criticality criteria and quantifiable and qualitative impacts on the organization arising from the loss of systems availability, integrity or confidentiality.
- Use security risk analysis methods, tools and techniques as appropriate to identify potential exposures to application systems critical to the continuity of the organization's business e.g. single point of failure, lack of effective countermeasures or lack of tested up-to-date recovery plans.

6.5.3 WHEN PROVIDING SYSTEM ADMINISTRATION AND OPERATIONS

- Adopt a policy that minimize the replenishment of consumables (in particular paper, cartridges) and enable recycling of those consumed.
- Proactively seek to improve the performance of the system (in particular databases, networks) by regularly monitoring responsiveness and tuning performance parameters accordingly.
- Regularly monitor resource usage and failure rates and keep management informed of any trend.

6.5.4 WHEN PERFORMING DATABASE ADMINISTRATION

- Beware of the commercial sensitivity of the organization's data,

taking measures to prevent unauthorized access, without preventing access by legitimate users.

- Enforce strict partitioning between operational data and data used for training or test purposes; discourage support staff from attempting any testing in the operational data.
- Make yourself aware of the licensing conditions and prevent situations where they could be breached.

6.5.5 WHEN MANAGING IT ASSETS

- Establish a management policy that states the organization's commitment to safeguarding its IT assets and promote awareness of this policy within the organization and to your customers and suppliers.
- Assign responsibilities for the purchasing, receipt, installation, movement and ultimate disposal of all IT assets, ensure that records are kept at each step.
- Establish mechanism to protect the organization's IT assets from external violation, use a combination of software controls (firewalls, virus protection, passwords) and physical controls.
- Promote awareness of the ethical and legal issues involved in having obscene material on an IT system.
- When it is necessary to download software, do so only with the permission of the owner.

6.6.0 SUPPORT AND MAINTENANCE

This section deals with establishing and managing a support service, and investigating problems.

6.6.1 WHEN ESTABLISHING A SUPPORT SERVICE

- Establish the level of support which may realistically be expected and provide the tools, documentation and suitable trained staff to meet this expectation.
- Promote a mechanism to change the level of service without the customer incurring excessive costs.
- Ensure the documentation of the supported systems and software is available and in an appropriate form for those receiving the call for support.
- Maintain a log of support requests and solutions; maintain a list of frequently asked questions.

6.6.2 WHEN MANAGING A SUPPORT SERVICE

- Identify to the customer any change to his business procedure that will improve the efficiency of the service provided, even if this will result to reduced revenues to his organization.
- Provide the customer with as much notice as possible of any change in the services level which may cause costing thresholds.
- Honestly maintain metrics on the services provided, resisting the temptation to hid shortcomings to came matrices look better, and take position measures to improve the services.

6.6.3 WHEN INVESTIGATING PROBLEMS

- Avoid unnecessary work by researching previous problems and looking for common solutions.
- Where similar problems re-occur, investigate ways of eliminating them, through system operational changes or additional training.

- Be aware of the commercial sensitivity of operational data; keep control of copies of such data and ensure destruction when the investigation is complete.
- Appreciate the consequences of making changes to operational systems: Resists the temptation to make adhoc fixes unless you are certain they will work.
- Be aware of the cost of investigation, especially when using remote communications links.

6.6.4 WHEN LAISING WITH DEVELOPMENT STAFF (INTERNAL OR THIRD PARTY SUPPLIERS)

- Do not hand over commercially sensitive information without ensuring that procedures for the handling, processing, storing and destruction of the information are in place.
- Ensure that you are included in any direct communication between the user and the development staff.

7.0 CASE STUDY.

8.0 CONCLUSION

The Code of Professional Practice for Information Technology Profession in Nigeria is established on four main Obligations: to the Public; the Employer or Client; Fellow members and; the Profession. The section on the Profession clearly states the importance of honouring property rights including copyrights and patents, trade secrets, terms of license and agreements. It further emphasizes respect for privacy of others and privacy of data describing individuals. It is instructive to note that CPN is

presently working to update the Code of Ethics and Professional Conduct of The IT Profession in Nigeria.

It is mandatory that every professional is conversant with his/her obligations and commits himself/herself in writing by signing below the closing statement of the Code:

“I commit myself to these aforementioned obligations, in fulfillment of my professional duties as a personal responsibility and as a member of the Profession. I shall actively discharge these obligations, and I dedicate myself to that end.”

Thank you

The END

ACKNOWLEDGEMENTS

- 1. Computer Professionals Registration Council of Nigeria, Code of Ethics and Professional Practice (2001)**
- 2. Computer Society Nigeria(Formerly Computer Association of Nigeria, Code of Ethics, Conduct and Practice for Computer Professionals.**
- 3. Computer Security: Jae K. Shim et al**
- 4. British Computer Society: Code of Practice**
- 5. British Computer Society: Code of Conduct**
- 6. Institute of Medical Illustrators: A Code of Professional Conduct for Members**
- 7. Australian Capital Territory, Canberra 2006: Teacher's Code of Professional Practice**
- 8. North Carolina Educators: Code of Professional Practice and Conduct**
- 9. The Certificate Board for Music Therapists: Code of Professional Practice**
- 10. Institute of Scientific and Technical Communication (2006): Code of Professional Practice.**
- 11. Recruitment and Employment Confederation (REC): Code of Professional Practice**

- 12. Australian Computer Society Code of Ethics**
- 13. Association for Computing Machinery (ACM): Code of Ethics and Professional Conduct**
- 14. Illinois Institution of Technology: Centre for study of Ethics in the Professions: Codes of Ethics ONLINE**
- 15. Institute for Certificate of Computer Professionals (ICCPP: Code of Ethics, Conduct and good practice for certificate Computer Professionals**
- 16. Data Processing Management Association: Code of Ethics**