



IITPSA CODE OF GOOD PRACTICE

JULY 2021

IITPSA NPC
P O Box 1714, Halfway House, 1685

IITPSA Code of Good Practice

1. Preamble

Any code may be considered as a formalisation of experience into a set of rules. A code is adopted by a community because its members accept that adherence to such rules, including the restrictions this implies, is of benefit to all, inside and outside the community alike. A code also has an educational role, by setting out what is required of those wishing to join the community.

It may be said that everything contained in an acceptable code is obvious and merely common sense. This, however, does not lessen its worth. The conscious selection and emphasis of a group of “common sense” items based on experience is by itself a worthwhile exercise.

The Code of Good Practice provides guidelines for all members of the IITPSA as they exercise their professional competence and carry out their work, and complements its companion, the IITPSA Code of Ethics which deals with ethical behaviour.

The two Codes apply to all members of the Institute, and especially to holders of professional designations. Because they are the distillation of considerable experience, they set standards for all engaged in the Information and Communications Technology (ICT) profession. At a time when ICTs are playing an ever-increasing part in national life, whether in business, industry, or social affairs, it is important for the profession to state clearly what its rules are.

2. Terminology:

The following conventions shall apply to the reading of this Code:

1. “Member” includes all categories of corporate membership defined in the Institute’s Memorandum of Incorporation and associated Rules.
2. “Client” is any person, department, or organisation for whom the member works, or undertakes to provide computer-based, or digital technology-based aid, in any way.
3. “User” is any person, department or organisation served by computer-based or digital systems.
4. “System” means all applications involving the use of computer and information technology. The term does not imply any particular mode of processing, e.g., local batch or remote real time, etc. “System” may be interpreted as encompassing non-computer procedures and disciplines, e.g., clerical, manual, etc.

3. Introduction and Explanation

This Code of Good Practice is directed to all members of IITPSA (Institute of Information Technology Professionals South Africa). However, in practical terms it is aimed specifically at the holders of professional designations of the Institute since they are expected to be exercising roles of responsibility at the level to

which the Code applies. It consists, essentially, of a series of statements that prescribe minimum standards of practice, to be observed by members.

The Code is concerned with professional responsibility. All members have responsibilities – to clients, to users, to the State and to society at large. Those members who are employees also have responsibilities to their employers and employers' customers, and sometimes to a Trade Union. In the event of an apparent clash in responsibilities, obligations, or prescribed practice the Institute should be consulted at the earliest opportunity.

The Code should be viewed as a whole: individual parts are not intended to be used in isolation to justify errors of omission or commission. Furthermore, the Code is intended to be observed in the spirit and not merely to the word.

IITPSA membership covers all occupations relevant to the use of Information and Communications Technologies and it is not possible to define the Code in terms directly relevant to each individual member. For this reason, the Code is set out in two levels to enable every member to reach appropriate interpretations:

Level One is a series of brief statements defining the elements of practice to be observed (and appears in the left-hand column below)

Level Two is the rationale for the Level One statements (and appears in the right-hand column below).

Level Two is not intended as guidance on how to carry out the Code of Good Practice, but only to provide an explanation of its meaning and the reason for the inclusion of the statement at Level One.

Where examples are given on how to apply the Code, these are simply to clarify the meaning. Many of the clauses may seem to state the obvious, but much that goes wrong in ICT use does so because the obvious has been overlooked.

4. Code of Practice

In the practise of their profession, members (to the extent that they are responsible) shall:

	LEVEL ONE (Statement)	LEVEL TWO (Rationale of Statement)
4.1	Personal Requirements	
4.1.1	Keep themselves, and subordinates, informed of new technologies, practices, legal requirements and standards as are relevant to their duties.	Others will expect you to provide special skills and advice and, in order to do so, you must keep yourself up to date. This is true for members of all professions, but particularly so in Information and Communications Technology which is developing and changing rapidly. You must also encourage your staff and colleagues to do the same, as it is impossible to retain your professional standing by relying only on the state of your knowledge and competence at the time you achieved professional status.
4.1.2	Ensure subordinates are trained on an equal opportunity basis, to be effective in their duties and to qualify for increased responsibilities.	You should regularly review the training needs of your staff and take action to ensure that your hard-won knowledge and experience is passed on in such a way that those who receive it not only improve their own effectiveness in their present positions but also become keen to advance their careers and take on additional responsibilities.
4.1.3	Accept only such work that they believe themselves to be competent to perform and will not hesitate to obtain additional expertise from appropriate qualified individuals where advisable.	You should always be aware of your own limitations and not knowingly imply that you have competence you do not possess. This is of course distinct from accepting a task for which successful completion will require additional expertise to your own. This point is central to the IITPSA Code of Ethics and the Code of Good Practice: you cannot possibly be knowledgeable on all facts, but you should be able to recognise when you need additional expertise and information and know where to find it.

4.1.4	Actively seek opportunities for increasing efficiency and effectiveness to the benefit of the user and of the ultimate recipient.	Whatever the precise terms of your brief, you should always be aware of the environment surrounding it and not work solely towards completion of the defined task and no more. You must regard it as part of your duty to make your client aware of other needs that emerge, unsatisfactory procedures that need modification and benefits that might be achieved. You, as an innovator, should consider the relevance of new methods and should always be looking for the possibility of additional benefits not foreseen when the project was planned. You must also look beyond the immediate requirements to the needs of the ultimate user. For example, the Invoice your system produces may be right for company accounting procedures but confusing for the person who is being expected to pay against it.
4.1.5	Impartiality	A member will act with impartiality when purporting to give independent advice and will disclose any relevant interests or conflicts.

4.2	Organisation and Management	
	<p><i>This section of the Code is concerned with broad principles. Management of development is covered in detail in Sections 5 and 6; management of operational projects in Section 7. Since ICT management is still management, the normal principles applicable to any kind of management also apply here.</i></p>	
4.2.1	<p>Plan, establish and review objectives, tasks and organisational structures for themselves and subordinates, to help meet overall objectives.</p>	<p>It is dangerously easy for you, as an ICT professional, to become fully engrossed in the problem of the moment, and to lose sight of the overall objectives of the organisation. ICT, no less than any other discipline, is an organic component of the organisation, and you should continuously ensure that the path you are following is in line with the objectives of that organisation. You must make use of the well-established management practices of monitoring and review to ensure the area of work for which you are responsible is making its maximum contribution.</p>
4.2.2	<p>Ensure that any specific tasks are assigned to individuals according to their known ability and competence.</p>	<p>When delegating work to your sub-ordinates, ensure that as far as possible the task will develop their competence and increase their motivation. However, you must also ensure that the principles implied in 1.3 are observed or you will be faced with dissatisfied users who are not receiving the service to which they are entitled.</p>

4.2.3	Establish and maintain channels of communication from and to seniors, equals and subordinates.	It is often assumed that communication will look after itself, but good communication is vital to business success. You must ensure that formal channels of communication exist upwards, downwards, and sideways in the organisation for which you are responsible. It is difficult to over- emphasise this point in connection with ICT work which by nature requires constant interaction between the members of the ICT organisation and, most importantly, with the users. Furthermore, you will find that communication skills can be improved considerably by formal training, and this should be included in your training plans as a high priority item.
4.2.4	Be accountable for the quality, timeliness and use of resources in the work for which they are responsible.	High on your list of professional duties will be the requirement to provide a service of agreed quality, on time and within budget. Beyond that, of course, is the requirement for contingency planning and the need to make others affected aware of difficulties and dangers if these are foreseeable. For this you, as a professional, are responsible. You cannot turn your back on a problem once encountered, and hope someone else will solve it or that it will simply go away. Action taken to minimise the impact of such problems will, in the end, ensure a smoother running organisation.

4.3	Contracting	
	<p><i>This section is included in the Code because some formal agreement – even if not a specific contract – is needed before any project is started. Commitment and definition of responsibilities are essential, in advance of action.</i></p>	
4.3.1	<p>Seek expert advice in the preparation of any formal contract.</p>	<p>In the same way as you would expect to be consulted in your field as an ICT professional, be ready to consult other specialists when you need guidance in drawing up contracts or in matters such as commerce, finance, tax, law or risk evaluation. Much of your time can be saved in this way, to say nothing of avoiding the potential dangers of a badly drawn up contract or wrong assessment of a legal situation. Many of these areas have become defined as standard practice and a number of professional bodies provide “standard contract” forms as a guide to their own members, which helps considerably to reduce problem areas.</p>
4.3.2	<p>Ensure that all requirements and the practical responsibilities of all parties are adequately covered in any contract or tendering procedures.</p>	<p>In the same way as you would carefully review the completeness of the detail for a system specification, it is necessary to review the totality of the detail to be covered by a contract. Take care to ensure that such items as provision of accommodation, typing, data preparation, responsibility for media security and standby arrangements are not forgotten. Apart from the problems which will arise if these things have been overlooked, the profitability of your contract will be adversely affected. Again, communication enters into this as you need to ensure that everyone who is party to the contract is fully aware of his obligations.</p>

4.4	Privacy, Security, and Integrity	
	<p><i>A system is at risk from the moment that the project that develops it is first conceived. This risk remains at least until after the system is finally discontinued, perhaps indefinitely.</i></p> <p><i>Threats to security range from incompetence, accident and carelessness to deliberate theft, fraud, espionage or malicious attack.</i></p>	
4.4.1	<p>Ascertain and evaluate all potential risks in a particular project with regard to the cost, effectiveness and practicality of proposed levels of security.</p>	<p>One of your more difficult responsibilities is that of determining the value of a system in terms of what would be lost if security was to be breached (e.g. damage to national security by leaks of military data, personal privacy by leaks from medical records or fraud by access to financial information). However, a view is required to aid decision making, covering how much should be spent on system security in at least these four areas:</p> <ul style="list-style-type: none"> • protection - preventing threats from becoming reality. • detection - in time to take suppressive action. • suppression – to limit the effect. • recovery - to rectify and get the system going.
4.4.2	<p>Recommend appropriate levels of security, commensurate with the anticipated risks, and appropriate to the needs of the client.</p>	<p>You still need to remember that you must give attention to some areas of risk which are mandatory such as those covered by legislation for health and safety at work. However, risks exist in connection with the security and people, all of which should be identified and recommendations made.</p>
4.4.3	<p>Apply, monitor and report upon the effectiveness of the agreed levels of security.</p>	<p>Situations are always changing and people are liable to become lax in observing routine practices. You will therefore find an on-going security audit extremely valuable in keeping people aware of security requirements and procedures, and in the identification of</p>

		weaknesses and loopholes in the security system. Moreover, security arrangements should be reviewed periodically in light of developing technology and the new methods of breaching security.
--	--	---

4.4.4	Ensure that all staff are trained to take effective action to protect life, data and equipment (in that order) in the event of disaster.	Naturally, the safety of people is your first priority, and the proper backup facilities for recovery of data files should exist. Equipment should be replaceable and normally insured. Your staff should be trained to react with regard to these priorities. Damaging a data processing centre will usually result in serious consequential losses to the business of the organisations involved. As a professional, you will be concerned to treat security drills as a serious matter and carry them out regularly. Everyone involved should be trained to be on the lookout for anything unusual.
4.4.5	Take all reasonable measures to protect confidential information from inadvertent or deliberate improper access or use.	Your responsibility for confidentiality of information is at least as great as that of members of other professions. The job is even more complex by reason of the speed, capacity and facility for data exchange by computers. Frequently, personal information will be under your control, and you should always be aware of the spirit and letter of relevant legislation and guidelines written to protect the individual.
4.4.6	Ensure that competent people are assigned to be responsible for the accuracy and integrity of the data in the data files and each part of an organisation's database.	You must take direct action to give responsibility to specific individuals to ensure the accuracy and integrity of data within each system. Whilst this is important for any system, however simple it becomes even more significant in more complex databases and communications environments.
4.4.7	Ensure that, where data is stored which maybe sensitive (or even dangerous) to an individual, the individual concerned has adequate rights of review, correction and appeal.	Computer databases often contain information which can seriously impact the freedom of action of private individuals. A frequent example is the storage of credit information. Situations will occasionally arise where this information is incorrect, or where it may be subject to different viewpoints, such as where an account is unpaid because of a legitimate dispute. In these situations, procedures should be developed to allow the affected person to review the information held in the database and, if such person believes it to be incorrect, to

		<p>have it rectified or at least to have his viewpoint incorporated. This protection becomes even more important when data obtained for one purpose (or by one organisation) is used for another purpose (or by other organisations).</p>
--	--	---

4.5	Development	
	<p><i>“Development” in this context means not only all the work involved in order to reach the stage where a viable computer system is ready to become operational; it also includes all the activities involved in installing the system in its eventual production environment.</i></p>	
4.5.1	<p>Exercise impartiality when evaluating each project with respect to its technical, moral and economic benefits.</p>	<p>Your responsibility in a project will give you opportunities to make decisions based on your personal views and preferences. The line between personal bias and professional opinion becomes somewhat finely drawn. To avoid finding yourself on the wrong side of the line, always make sure you are aware of your client’s objectives and the benefits he/she is looking for, and be careful not to lose objectivity through enthusiasm created by the latest technological developments.</p>
4.5.2	<p>Effectively plan, monitor, adjust and report on all development, acquisition or replacement projects.</p>	<p>This principle is no different from that applying to many other fields, but your attention is drawn to it as it is essential to business control in any organisation.</p>
4.5.3	<p>Ensure that effective standard procedures and documentation are available and used.</p>	<p>A characteristic of professionals is that they depend on the operation of a series of standards and procedures for efficiency and professional results. You should ensure that the standards you lay down do not cause inhibiting rigidity, but provide a framework within which individuals know how, when and by whom the work is to be done.</p>

4.5.4	Specify the system objectives, completion date, cost and security requirements for the client and the necessary criteria for their achievement.	Always ensure that you produce a clear statement with qualified objectives wherever possible which can be agreed to with the client. It is all too easy to overlook this point in the general rush of business life: when committing agreements to paper it is frequently a neglected activity. For large projects covering a significant span of time, objectives should in fact be regularly reviewed to ensure that the project is still relevant in the light of changing circumstances.
4.5.5	Ensure that the client can participate in all stages of problem analysis, system development and implementation.	The system you develop ultimately belong to your client, and therefore he/she needs to maintain control and be given opportunities to exercise them. Therefore you should seek his/her involvement in key project activities, e.g. the specification, quality control and provision of test data. You should encourage and help the client to achieve the right level of involvement not less because in this way you ensure that you produce the system that the client requires.
4.5.6	Ensure that each task is completed to a defined level before the next dependent task is started.	A task may be anything from specifying a system to determining the size of a piece of detailed code. While many tasks will be executed in parallel, dependent tasks should be completed sequentially with non-dependent activities within them overlapped. For example, you should not start writing a program in advance of a complete specification if you wish to avoid duplication or loss of effort.
4.5.7	Specify and conduct program tests and system tests to ensure that all system objectives are met to the satisfaction of the client.	It is clearly necessary for you to test each program separately and then all programs together as a complete suite, followed by the computer elements together with the rest of the system. The objective is to prove the system functions as intended and not merely to detect errors. The client should be involved in the testing to achieve the objectives in 5.5.
4.5.8	Ensure that systems are designed and sufficiently documented to facilitate subsequent audit, maintenance and enhancement, and accurate comprehension	It is essential, at the originating stage, that you consider and provide for the needs of future audit and modification. Documentation should also assist troubleshooting and enable modification to be undertaken with minimal reprogramming and the smallest possible impact on operations. Also your users will require documentation in a convenient form to enable

	by users.	them to understand and properly utilise the system.
--	-----------	---

4.5.9	Ensure that input and output are designed to obviate misunderstanding.	The input and output of a system is normally prepared or received by non-technical users and consequently must be designed to simplify business life rather than add extra burdens. Input and output should be easily readable (avoid jargon, unfamiliar codes and abbreviations) and provide clear headings and such things as page numbers. Whenever possible, the power of the computer should be used so as to permit the maximum use of plain language.
4.5.10	Ensure that there are adequate procedures available to delete erroneous, redundant and out of date data from files.	It is part of a sound approach to consider not only the immediate use of a system but also its effectiveness during a life which will be as long as it continues to meet its objectives. During this life, redundant data is bound to accumulate and it will be essential to periodically remove such data. Also due, to system weaknesses and clerical procedures, undisciplined corrections or deletions may occur, thereby compounding the problem, and possibly resulting in the system producing erroneous results.
4.5.11	Ensure that adequate procedures are available which will, with the minimum of inconvenience, restore data files and program files to their required conditions in the event of data loss, corruption or system failure.	This is complementary to 4.1. The design stage is the time to ensure that the restorative procedures are incorporated. When an operational disaster occurs it will be too late to start thinking about such procedures. <i>(The emphasis in 5.10 and 5.11 is for clear procedures to protect data and programs from corruption rather than relying on ad hoc correction by individuals who may subsequently be the only ones who know what they have done.)</i>
4.5.12	Ensure that projects are completed with technical soundness, using the most appropriate technology and within time and cost constraints.	Cost and service are criteria of an effective system rather than technical ingenuity. The technology to be exploited should be the best for the client's problem not necessarily the most sophisticated.

4.6	Implementation	
	<i>The term is used here to describe the transition from development to full operation.</i>	
4.6.1	Ensure that adequate provision is made for user and operations staff training in all functions of the system for which they are responsible.	<p>You should not consider the task complete until you have seen the new system through to implementation. Your professional duty requires you to see that the system can be used effectively by your client's staff.</p> <p>Each new system will bring with it, to some degree, new approaches, new techniques and new ways of doing things.</p> <p>These have to be explained to your users who may show resistance to change because of their previous experience.</p> <p>You should recognise that they will require time to become familiar with the new system and to gain confidence and ability to meet the new conditions.</p> <p>Training in advance of implementation is normally essential to countering these problems.</p>
4.6.2	Effectively plan, monitor, adjust and report upon all activities concerned with the changeover from development to operational running.	<p>These are vital parts of the design and development process. Your plans should specify in detail all resources involved whether user's or ICT staff. Further constant reviewing will be necessary as implementation responsibilities will be put to the test here, as all who are affected will need to be advised of changes and be given the opportunity to comment. Again the opportunity presents itself to help generate the understanding, confidence and sense of involvement so necessary to successful implementation and subsequent operation.</p> <p>If you fail to carry out these functions effectively, operation dates will be jeopardised and, almost certainly, implementation costs will be higher than they need be.</p>
4.6.3	Ensure expeditious and economic completion of implementation consistent with adequate testing and security.	<p>Here you are involved in a professional judgement, or trade-off between under- and over-testing. If you cut corners by, say, reducing system testing time, then the likely effect on the operation elsewhere should be evaluated and made known to those who should know.</p>

4.7	Live Systems	
	<i>This section is concerned with the ongoing operation of systems handed over by design and development staff.</i>	
4.7.1	Plan and operate efficient and reliable processing within defined budgets.	“Processing services” covers all the activities between reception of data and delivery of results. You must ensure that these services are provided efficiently to users who are just as dependent on these as they are on the application software for the well-being of their business.
4.7.2	Monitor performance and quality and arrange regular reviews of the efficiency, effectiveness and security of live systems.	The dynamic nature of most business environments means that, over a period, a system may gradually provide the user with a system of reduced value and quality. Regular post-implementation reviews will be all the more effective if you check not only how well the system is meeting its original objectives, but also how it has evolved in the light of current business requirements.
4.7.3	Plan, from the start of a project, to provide adequate maintenance and enhancement support to live systems so that they continue to meet all requirements.	Much of the criticism computer applications receive is traceable to their failure to respond, by means of modification, to changing conditions. Either modifications do not happen, or they are implemented haphazardly over too long a period. If you ensure that your project plans include provision of a formal system to control the enhancement of programs, and identify the need for appropriate maintenance resources, you will avoid user dissatisfaction arising from this type of problem.
4.7.4	Establish good liaison with users and provide proper facilities for dealing with enquiries and day-to-day problems concerning the user of their systems.	One of the most important areas where your professional skill will be required is in maintaining continuous formal and informal liaison with your users. All those concerned with the services which you are responsible for providing should know and understand the need for formal channels of communication. In particular, do not forget to ensure that these exist to cover the special circumstances which arise in emergencies.