Policies and Procedures Manual
(Draft Only)
# CONTENTS

## CHAPTER 1 ORGANISATIONAL RESPONSIBILITY ......................................................... 1-1

1. POLICY .............................................................................................................. 1-1
   1.1. Organisational Responsibility Policy ......................................................... 1-1
2. STANDARDS RESPONSIBILITIES .................................................................. 1-1
   1.2. Standards Responsibilities Procedures ..................................................... 1-1

## CHAPTER 2 DOCUMENTATION PROCESS ............................................................. 2-1

1. POLICY .............................................................................................................. 2-1
   2.1. Policy ......................................................................................................... 2-1
2. FEASIBILITY STUDY/NEEDS ANALYSIS .......................................................... 2-1
   2.2. Feasibility Study Documentation Procedure ............................................ 2-1
3. PROJECT DOCUMENTATION ......................................................................... 2-2
   2.3. Project Documentation ............................................................................. 2-2
4. SOFTWARE DOCUMENTATION ...................................................................... 2-3
   2.4. Software Documentation ......................................................................... 2-3
5. COMPUTER OPERATIONS DOCUMENTATION .............................................. 2-4
   2.5. Computer Operations Documentation .................................................... 2-4
6. FLOWCHARTING STANDARDS ....................................................................... 2-6
   2.6. Flowcharting standards .......................................................................... 2-6

## CHAPTER 3 FINANCES ......................................................................................... 3-1

1. FINANCE POLICIES ........................................................................................ 3-1
   3.1. Finance Policies ....................................................................................... 3-1
2. PURCHASING PROCEDURES .......................................................................... 3-3
   3.2. Purchasing Procedures ........................................................................... 3-3

## CHAPTER 4 COMPUTER SOFTWARE .................................................................... 4-1

1. SOFTWARE POLICIES ..................................................................................... 4-1
   4.1. Software Policies ...................................................................................... 4-1
2. PURCHASING SOFTWARE .............................................................................. 4-1
   4.2. Purchasing Software ................................................................................ 4-1

## CHAPTER 5 IT EQUIPMENT .................................................................................. 5-1

1. IT EQUIPMENT POLICIES ............................................................................... 5-1
   5.1. Equipment Policies .................................................................................. 5-1
2. PURCHASING HARDWARE .............................................................................. 5-2
   5.2. Purchasing Hardware ............................................................................... 5-2
3. EQUIPMENT REGISTER (PROPOSAL) ............................................................. 5-5
   5.3. Equipment Register .................................................................................. 5-5

## CHAPTER 6 USE OF SYSTEMS ......................................................................... 6-1

1. E-MAIL POLICY ............................................................................................... 6-1
   6.1. E-mail Policy ............................................................................................ 6-1
2. INTERNET ACCESS POLICY .......................................................................... 6-2
   6.2. Internet Access Policy .............................................................................. 6-2
3. NETWORK ACCESS/SHARING POLICY ........................................................ 6-3
   6.3. Network Access/Sharing Policy ................................................................ 6-3

## CHAPTER 7 IT DEPARTMENT OPERATIONS ......................................................... 7-1

1. IT DEPARTMENT OPERATIONS POLICIES ................................................. 7-1
   7.1. IT Department Operations Policies ........................................................... 7-1
2. GENERAL OPERATIONS ............................................................................... 7-2
   7.2. General Operations .................................................................................. 7-2
3. OPERATING PROCEDURES .......................................................................... 7-4
   7.3. Operating Procedures .............................................................................. 7-4
4. IT TECHNICAL SUPPORT ............................................................................. 7-5
   7.4. IT Technical Support ................................................................................ 7-5
CHAPTER 8 IT SYSTEM SECURITY .................................................................8-1

1. IT SYSTEMS SECURITY POLICY .................................................................8-1
   8.1. IT Systems Security Policy .................................................................8-1

2. STAFF INDUCTION PROCEDURE ............................................................8-2
   8.2. Staff Induction Procedure .................................................................8-2

3. SECURITY ALTERATION PROCEDURES ..............................................8-2
   8.3. Security Alteration Procedures .......................................................8-2

4. VENDOR/CONTRACTOR ACCESS POLICY ...........................................8-3
   8.4. Vendor/Contractor Access Policy ....................................................8-3

CHAPTER 9 DISASTER RECOVERY (TO BE ADDRESSED) .........................9-1

1. DISASTER RECOVERY POLICY ...............................................................9-1
   9.1. Disaster Recovery Policy .................................................................9-1

2. DISASTER RECOVERY PROCEDURES .................................................9-1
   9.2. IT Systems Disaster recovery Procedures ......................................9-1

VERSION CONTROL

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change Outline</th>
<th>Completed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft 1.0</td>
<td>29/7/02</td>
<td>Initial Draft</td>
<td>Chris Morahan</td>
</tr>
<tr>
<td>Draft 1.1</td>
<td>15/10/02</td>
<td>First major Draft</td>
<td>Chris Morahan</td>
</tr>
<tr>
<td>Draft 1.2</td>
<td>23/10/02</td>
<td>Addition of Finance and Use of Systems Sections</td>
<td>Chris Morahan</td>
</tr>
<tr>
<td>Draft 1.3</td>
<td>29/8/03</td>
<td>Addition of Malicious attacks subsection 6.3.3</td>
<td>Chris Morahan</td>
</tr>
</tbody>
</table>
Chapter 1 Organisational Responsibility

1. Policy

1.1. Organisational Responsibility Policy

The purpose of the Policies and Procedures Manual is to provide a conformity instrument for the analysis, development, design, documentation, control of and software provision for information systems in the Colleges Information Technology Group (CITG).

1.1.1. Scope

This manual provides the guidelines for policies, systems and procedures related to information systems functions at network and standalone levels. It is not intended to replace instructions by various vendors in the operations of their software or hardware.

1.1.2. Policy Objectives

The policy objectives are to:

1. Differentiate between the network and the standalone computer operations.
2. Provide structure to the various information systems and to the relationship of network and standalone systems with the college’s operating environment.
3. Assign the responsibility and define the authority for controlling all computer and network standards, operating standards and training.

1.1.3. IT Systems

College information Systems or IT Systems shall be defined as: Computers & their peripherals, network infrastructure, data communications equipment and telephone systems excluding mobile telephony.

2. Standards Responsibilities

1.2. Standards Responsibilities Procedures

1.2.1. Source of Authority

Information systems policies will emanate from the highest level of authority of the Colleges that the computer procedures will affect.

The IT Manager is the authority for all college computer systems. He/she will receive policy mandates from CITG Committee. These policies will be defined in writing and dated, signed and forwarded to the IT Manager who will incorporate these policies, along with his/her own, into the information systems policies.

1.2.2. Policies and Procedures Responsibility

All computer operations, software, supplies and supporting hardware for colleges will be the responsibility of the IT Manager. The authority to enforce the “CITG
Policies and Procedures Manual” is provided by CITG Committee. The chairman of the CITG Committee has the responsibility to confirm approval and sign a master copy of all issued and all temporary policies and procedures.

1.2.3. Implementation

All management personnel of Colleges utilising computer systems managed by the CITG are responsible for ensuring that the provisions set forth in the “CITG Policies and Procedures Manual” are complied with. These management persons are responsible for:

1. Insuring that all application standards are followed in their respective areas.
2. Informing the person in charge of approving the procedures if there are any problems with a procedure or if inputs from other sources do not comply with the defined procedures. This should be done in the form of a memo.
3. Providing new employees with instruction and/or documented procedures that relate to their job descriptions.

1.2.4. Manual Maintenance

Manual revisions that are permanent will be sequentially identified, in the revisions section at the beginning of the manual. Temporary policies or procedures supersede permanent policies and procedures, which will remain in the manual in their assigned section and can only be replaced by the issuance of replacement policies and/or procedures. In the event that a policy and/or procedure is to be discontinued, an order will be issued in memo form by the person who originally approved the policy and/or procedure, or by a successor or agent. Requests for temporary or permanent policy and/or procedures will be handled as follows:

1. Any user, management person or manual holder can submit a request for a temporary policy and/or procedure or for a permanent revision to the “CITG Policies and Procedures Manual”.
2. Requests must be submitted using the “CITG Policies and Procedures Manual Revision Request Form” (ITS001).
3. Submit one copy to the approving authority (or successor) for the policy and/or procedure.
4. The approving authority will review the request and approve or deny in memo form citing a reason for whatever action is taken. The person assigned to investigate the request will be identified in the memo. The recommended course of action can result in a feasibility study if the required undertaking is large or expensive enough.
5. If the request is denied, the person requesting the change may appeal the decision.

The revised documentation is to be issued in the same manner as the original documentation to all affected manual holders. When permanent revisions are issued, all pages for the given section will be reissued. If corrections to current procedures are required and numbering is not affected, only the affected pages need to be distributed. This applies to both temporary and permanent policies and/or procedures. All releases will have a cover memo noting:

1. The person issuing the release
2. The effective date or dates of the release
3. The reason for the release.
The person responsible for maintaining the manual will keep a current list of all manual holders who will be identified as having a partial or complete manual. When a particular section is replaced, a list of appropriate manual holders can be provided for distribution. The manual may be maintained in electronic format, however notice of alterations as described above must still be sent. Each member College of CITG shall be supplied with one (1) Official hard copy of manual.

<table>
<thead>
<tr>
<th>Revision Request for Information Systems Policies &amp; Procedures Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Manual Area</td>
</tr>
<tr>
<td>Suggested Revision</td>
</tr>
<tr>
<td>Revision Rationale:</td>
</tr>
<tr>
<td>Signed</td>
</tr>
<tr>
<td>Comments</td>
</tr>
</tbody>
</table>
Chapter 2  Documentation Process

1. Policy

2.1. Policy

Documentation is a formal means of conveying information. It is a permanent record of operation methods, development techniques and organisational policies. Documentation provides the media for the recording of procedure development, design, implementation, operation and revision data. It incorporates policies, rules and information that must be distributed properly to all users associated with information systems operations so that energies are directed and coordinated correctly.

User documentation should be written following specific standards defining the content, approach and objectives. The standards provide a uniform plan for handling every aspect of documentation.

Information systems areas requiring policy and procedures documentation are:

1. Procedure development
2. Computer management operations
3. Computer users
4. Computer user support

A standard A4 binder should be used to contain the applicable policies and procedures. It is envisaged that an “on-line” version of the manual would be made available to all computer system users. The IT Manager should retain a complete printed copy of the manual, as should the Business Manager/Bursar of each College.

2. Feasibility Study/Needs Analysis

2.2. Feasibility Study Documentation Procedure

A feasibility study is conducted to determine the practicality of changing developing or acquiring a system or computer program. Such studies can be omitted when a project is mandated by the CITG Committee and/or outside regulatory agencies, or where the expected expenditure on the project is less than $5,000.00. Each feasibility study, which will consist of a small scale systems analysis and a feasibility report, will require a folder to contain documentation such as memos, correspondence, vendor literature and detail information.

The analysis section is a scaled down study of a current system and a determination of the practicality of the request. The feasibility report contains documented findings as to the request’s feasibility. The final feasibility study report is prepared based on these two sections and any other pertinent information.

2.2.1. Feasibility Study Request Memo

An authorised requesting memo or e-mail memo will initiate each feasibility study request. The requests can only be authorised by College Manager/Bursar level or above. The memo will state:
• The nature of the requested system or software.
• The expected tangible and intangible benefits from the new or revised system or software.
• The date by which a reply to the report is needed.
• The contact person for further information about the request.

2.2.2. Feasibility Study Folder Contents

If the approving authority denies the feasibility study request, a notification is sent to the person requesting the study, explaining the reason(s) why the request was not approved. Both the requesting and reply memos will be filed in a “feasibility reject file” in the area of the systems and procedures unit. When the request for a feasibility study is approved, a feasibility folder labelled with the title of the study will include the following:

• An accumulated table of contents.
• All memos related to the study.
• Vendor correspondence.
• Vendor literature.
• Accumulated costs data for the study.
• A log listing the calendar days and hours worked on the study.
• Documentation of all meetings.
• A telephone log regarding all phone calls made and attempted.
• A copy of the final report.

2.2.3. The feasibility Study Report

The final feasibility study report will include and be formatted in the following manner:

• Cover page, containing project title, author and date.
• Overview of request.
• Rationale for initiating the information systems project, or for changing the existing system.
• The body of the final report providing the details of the project/program.
• Any supporting documentation/exhibits.
• Summary, containing recommendations, estimated costs, estimated calendar time needed, and estimated man-hours of all persons involved in the project.

3. Project Documentation

2.3. Project Documentation

Project documentation includes instructions, charts a copy of the feasibility study, correspondence and other material dealing with a specific project. It provides a permanent description of the undertaking along with the solutions to problems and the methods used to resolve them.

When starting a project, a project binder is created to provide an ongoing record of information relating to the specific project. It should include all related material and vendor information and correspondence throughout the life of the project. At no time are the contents to be removed from the project documentation folder. If
necessary, a copy can be made of any needed part(s). These copies should be marked with the copy date and the word “Copy” on each page. Each item placed in the folder should have the date clearly marked on it to avoid problems with superseded information.

2.3.1. Identification and Responsibility
A project number and title are used to identify each project folder. Responsibility for initiating and maintaining the binder rests with the project leader/manager or other responsible person as designated by the IT Manager.

2.3.2. Contents of Binder
The binder of a proposed project contains:

1. Table of contents
2. Project proposal
   The project report may be in the form of a feasibility study, a systems design or it may specify software requirements. The project proposal should contain
   a. Description of the project (includes feasibility study)
   b. Major project tasks
   c. Estimated costs
   d. Time estimated for each task
   e. Project staffing (numbers and skill level required)
   f. Project contact personnel
3. Systems Concept
   A paragraph, or more, written for non-technical, management-level personnel, which provides a detailed overview of the project objectives.

2.3.3. Project Progress Folders
Project progress documentation folders, maintained during the life of the project, contain the history of the project and copies of all relevant correspondence filed by date. They also provide a complete historical record, which becomes a source of information when writing a project completion report and should reflect any agreements between the project group and users or vendors. The folder should include:

- Correspondence
  a. Memos and letters.
  b. Project status reports.
  c. Minutes of status and problem solving meetings.
- Manpower utilisation record
  This will usually take the form of the “Project resource Schedule”, any variations that reflect a cost of over $300 are to be explained in a memo form at the time of the actual expense posting.

4. Software Documentation

2.4. Software Documentation
Software documentation serves various functions. First, program maintenance has become a major expense. The investment and effort required to document software is
rewarded by reduced maintenance costs and possibly management job security. Program documentation provides the IT department and users the information needed to operate the software. It also furnishes the auditors with information about the controls that have been established. Finally it shows management what exactly has been accomplished with the money spent.

2.4.1. Software Folders
Information about developed programs and purchased software is maintained in “software folders,” one for each written program or purchased software package. They contain:

1. General information
   This section identifies the software and its objectives. Each program should have a unique identification number. The programs should be grouped together into categories such as:
   - Operating software
   - Database software
   - Network software
   - Purchased workgroup software

2. General objectives
   The general objectives include a brief narrative statement of each program’s purpose or use.

3. Purchased software
   Any licence agreements connected with the programs. Including the number of copies purchased and the last date of purchase. Any “Beta” software will be so identified and its agreement information placed in this section.

4. Written program documentation

2.4.2. Backup and Recovery
Programs tend to be updated regularly, when this is done, all changes are to be noted with the date and the name of the person responsible. Each program must have a recovery procedure in the event of a computer failure. Each backup procedure will be tested after it is placed into operation and whenever maintenance has been performed. Backup procedures require the following:

- When and how the backup was done
- The location where backup programs and data are stored
- The number of backup generations required. If more than one, they should not all be stored in the same location.
- If an outside backup facility is available, a complete written procedure is required for its operation.

5. Computer Operations Documentation

2.5. Computer Operations Documentation
The operating procedures necessary to initiate, schedule, process, control and restart all phases of the system(s) while it is in operation are maintained in a folder for the operations personnel. All the documentation must be kept current. The project
leader is responsible for compiling and validating new systems. Maintenance
information systems personnel must update existing manuals.

The IT Manager has responsibility for systems manual maintenance and accepting
any new procedures into the manual. The authorised person notes the acceptance of
documentation on the upper right corner of each procedure sections first page.

2.5.1. Network Computer Systems

This section deals with the information systems operations procedures for the
College’s network systems. It covers general information pertaining to the overall
network system(s), backup and recovery and job procedures.

1. General Information
   Includes a narrative description of the overall operation, the system hardware,
   operating system, the purpose of the system and the methods used to accomplish
   the tasks. The users of this documentation are CITG operations personnel.

2. Backup and Recovery Procedures
   Documented by CITG and checked by Colleges. Included in these procedures are:
   • A list of who has what authority.
   • Backup and recovery on-site procedures
   • Backup and recovery off-site procedures
   • Disaster plan procedures

3. Computer Operation Procedures
   Job instructions should include the following
   • Job set-up instructions
   • The sources and media used for all data
   • Samples of any output (screens and printed material)
   • Corrective action to take for error messages
   • Expected run time
   • Logging procedures
   • Contact details in case of problems
   • Timetable of run times

2.5.2. Stand-alone Computer Systems

Stand-alone computers or systems that are not connected to the College Networks
fall into this category. These are systems found throughout colleges and may not have
any relationship to other computer systems. However, to maintain order, consistency
and a higher level of overall efficiency, their documentation process requires a central
source. CITG has the responsibility for college-wide information systems
documentation, maintenance, policing and training, as well as help desk operations for
the procedures issued.

1. Stand-alone general information
   The general information part of this documentation should apply to all users of
   independent microcomputers throughout the Colleges, and should include the
   following information item:
   • Corporate policies governing microcomputers.
   • Basic operations, password, etc.
   • Daily housekeeping procedures.
   • Accessing needed programs or data.
• Getting on the network.
• Contact person for problems.

2. Stand-alone operation procedures
The information in this module will vary from computer to computer depending on their use. The following items should be considered for each module:
• Hardware/software vendor documentation.
• Backup and retention procedures.
• Corrective action for common error messages.

6. Flowcharting Standards

2.6. Flowcharting standards
Flowcharts are to be used to depict the logical flow of events or operations steps within a procedure. Flowcharting is useful for illustrating manual office procedures and is easy to follow, even by people outside the Information Systems area. The flowchart shows operation steps and logic decisions to be followed by the user for a given situation. All the symbols used should conform to the ANSI standards. These symbols are shown in Exhibit 2-1. Follow these rules in preparing flowcharts:

1. Draw charts on A-3 or A-4 Paper
2. Charts should be drawn using charting software such as Microsoft Visio™, so that the manual may remain in software document format.
3. The general direction of the flow is top to bottom and left to right.
4. When the flow is not specified or whenever increased clarity is desired, use arrows to indicate the direction of flow.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>This symbol represents a processing function.</td>
</tr>
<tr>
<td>Decision</td>
<td>This symbol represents a decision step, with one or more alternative paths to be followed.</td>
</tr>
<tr>
<td>Document</td>
<td>This symbol represents a printed document output</td>
</tr>
<tr>
<td>Terminator</td>
<td>This symbol is used to start or stop a flowchart</td>
</tr>
<tr>
<td>Annotation</td>
<td>This symbol is used for adding comments to an operation</td>
</tr>
<tr>
<td>Flow Lines</td>
<td>Flow lines are used to connect the symbols and show the process flow.</td>
</tr>
<tr>
<td>Predefined Process</td>
<td>This symbol is used to illustrate a sub-routine or process that is defined elsewhere.</td>
</tr>
</tbody>
</table>

Exhibit 2-1
Chapter 3  Finances

1. Finance Policies

3.1. Finance Policies

This section sets down policies used to ensure that CITG finances are handled appropriately, and remain open and accountable. This section covers procedures to insure accountability throughout the finance system. These procedures are designed to ensure that the management and audit policies of the member Colleges will be satisfied and to support their enforcement.

3.1.1. Delegation of Authority

All purchases of software, supplies and supporting hardware for colleges will be the responsibility of the IT Manager. The authority for this purchasing is provided by CITG Committee. The chairman Of the CITG Committee has the responsibility to confirm approval and sign a copy of any purchasing documentation that exceeds the sole purchasing limits of the IT Manager.

Payment of accounts is the responsibility of the CITG treasurer. The authority for this is provided by the CITG committee.

3.1.2. Purchase Limits and Payment Methods

<table>
<thead>
<tr>
<th>Purchase/Payment Method</th>
<th>Purchase Value</th>
<th>Delegated Signatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Cards</td>
<td>&lt;$500</td>
<td>IT Manager</td>
</tr>
<tr>
<td>Reimbursement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase Orders</td>
<td>$500 - $10,000</td>
<td>CITG Chairman</td>
</tr>
<tr>
<td></td>
<td>$10,000 – $20,000</td>
<td>Passed at Meeting</td>
</tr>
<tr>
<td>Tender / Contract</td>
<td>$20,000 +</td>
<td>CITG Chairman</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Passed at Meeting</td>
</tr>
</tbody>
</table>

The method chosen should be appropriate to the nature and value of the goods and services required.

3.1.3. Authority to Purchase

The Authority to Purchase is vested in nominated positions as outlined in the “Purchase Limits and Payment Methods” policy.

The CITG Committee outlines the procurement action that must be followed depending on the level of expenditure involved.

<table>
<thead>
<tr>
<th>Cost</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $1,000</td>
<td>No quotes Required</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>$1,000 less than $5,000</th>
<th>As a minimum obtain three (3) quotations. (Verbal quotations are acceptable provided full details of date, company, contact person, and price is recorded and staff obtaining signs record)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5,000 less than $20,000</td>
<td>Three (3) written quotations</td>
</tr>
<tr>
<td>$20,000 +</td>
<td>Call Formal tenders</td>
</tr>
</tbody>
</table>

All costs are inclusive of Goods and Services Tax (GST)

**Special Conditions**

- Where a University of Queensland Contract is in existence covering goods and services, CITG may purchase under that Contract without seeking quotes. Procurements under University Purchase Contracts with a value in excess of $20,000 must still be referred to the CITG committee to determine whether Tenders should be called.

**3.1.4. Corporate Credit card**

The CITG Corporate Credit Card was introduced as an alternative purchasing and payment mechanism to improve payment performance, simplify clerical processes, provide more effective cash management and in many cases better service delivery. The card system is specifically designed for, but not restricted to, high volume but low value (less than $500) transactions.

Corporate Credit Cards are for official business purposes only. Misuse of cards will result in revocation and may result in disciplinary action being taken by the University.

**3.1.5. Conflict of Interest and Ethical Behaviour**

Guidelines pertinent to staff involved in procuring goods and services on behalf of the University are set out below:

- Staff members should avoid any financial or other interest or undertaking that could directly or indirectly compromise the performance of their duties. They should assess potential conflicts of interest in terms of the likelihood of their being influenced or appearing to be influenced in the performance of their duties in a particular matter.

  When staff members become aware of such a situation, they should take appropriate steps to disclose the conflict and may discuss it with senior staff who may offer advice.

- No staff member should accept a gift or benefit if it could be considered by the public, knowing the full facts, as intended or likely to cause the staff member to do his or her job in a particular way, or to deviate from a proper course of duty.
It is expected, however, that token gifts or benefits may be accepted provided there is no possibility that the recipient might be, or might appear to be, compromised in the process or where the gift could be seen by others as either an inducement or reward which might place a staff member under an obligation.

- Where staff members have access to official CITG documents and information in the course of their employment, they need to maintain confidentiality and privacy of that information in order to protect individuals concerned and to ensure the efficiency and effectiveness of the operations of the Colleges. In general, staff members should only disclose official information when required to do so by law, when the need arises as part of their normal duties, when they are called upon to give evidence in court, or where the information has been officially approved for release.

### 3.1.6. Goods and Services Tax

CITG pays GST on all goods and services purchased. Where CITG activity using the goods and services is classified as 'GST Free' an input tax credit is claimed back from the Tax Office on a quarterly basis.

### 3.1.7. Leasing vs. Buying

Any decision to acquire assets via rental or lease requires a full cost benefit analysis.

Whilst there are tangible benefits from leasing in relation to avoiding the risk of obsolescence and resultant poor resale value for items purchased outright (particularly in relation to IT equipment), due consideration should also be given to the 'hidden' costs of leasing. These hidden costs can include;

- penalties for early termination of lease
- administrative costs of periodic lease payments
- costs associated with negotiating and executing lease agreements

The delegated authority to approve agreements between CITG and an external party involving any borrowing, debt financing, hedging, sale and lease back, or similar financing arrangement is vested in the CITG Committee.

## 2. Purchasing Procedures

### 3.2. Purchasing Procedures

Procedures for gathering quotations and purchasing equipment should not be so restrictive in their nature so as to significantly hamper the purchasing process, or cause undue delays where equipment/services are required. It is important however that the procedures stand up to any external scrutiny with regards to competitive and ethical behaviour.
3.2.1. **Quotations (Quotes)**

Quotations are statements of the current market price of goods and services offered by interested parties and are usually valid for a specified period.

**Requesting Quotations**

When requesting quotations those invited to quote should:

- all receive the request at or about the same time
- all receive the same information
- represent a fair selection of available providers

**Procurements where the value exceeds $1,000 but is less than $5,000** – The IT Manager must ensure that as a minimum, three (3) quotations are obtained (and recorded). These quotes may be verbal, they shall however, be recorded and included in the documentation submitted to the approving officer with Delegation to approve the procurement. This will facilitate comparison and approval as well as meeting probity and audit requirements.

**Procurement or agreement where the value exceeds $5,000 but is less than $20,000** – The IT Manager must ensure that three (3) written quotations from reputable suppliers for the procurement. Quotes should be in writing and may be received in person, by facsimile or mail.

**For procurements exceeding $20,000 but less than $100,000** – The IT Manager should call prepare and call for a formal tender for the supply of the Goods and or Services. This tender is to be dealt with in line with the Tender policies of the University of Queensland.

In normal circumstances Centres will be expected to accept the lowest written quote unless it does not meet the standards specified in the call for quotations.

If less than the required number of quotes is received, the reasons for not inviting more quotations should be documented e.g. critical time restraints.

**Bid Shopping** - staff must not enter into any process of unfairly trading off different quotations in an attempt to seek lower prices.

3.2.2. **Purchases below $1,000**

For procurements below $1,000 quotes are not required providing:

- that the rates are reasonable and consistent with market rates for items of a similar nature
- required goods and services are not split into components or a succession of orders for the purpose avoiding the requirement to call for quotations
- fairness, equity and ethical dealing are assured.

3.2.3. **Purchase Orders**

**Purchase Order** - A Purchase Order is CITG’s official contractual form issued by the IT Manager - Purchasing to procure goods and services on behalf of the CITG. Purchase Orders are raised only for items to be used by CITG and cannot under any circumstances be used for staff or student personal requirements.
Purchase orders are created using the CITG Finance software, and are only valid once signed by the delegated authority.

**A Purchase Order is required for all asset purchases and for goods and services over $500 in value** and for smaller value orders when other means are not appropriate.

**Confirmation Orders** - the ordering of goods / services without a purchase order, where policy dictates a purchase order must be used, will only be accepted in cases of emergency such as equipment breakdown and storm damage repairs. Such circumstances still require the creation of an appropriately approved Purchase Order with the IT manager. Such orders will be endorsed as 'Confirmation Orders'.

**Order Cancellation** - The cancellation of a previously placed Purchase Orders can only be actioned by the IT Manager. The IT Manager will confirm cancellation in writing with the supplier.

**Variations to Orders** - Variations to a previously placed Purchase Order can only be actioned by the CITG Treasurer. Requests for variation should be made by way of a signed memo clearly indicating what changes need to be made and the reasons for the changes. A 'revised' Purchase Order will be created by the CITG Treasurer.

**Order Splitting** - Requisitions for required goods and services must not be split into components or a succession of orders for the purpose avoiding the requirement to call for quotations or tenders.

**3.2.4. Receiving of Orders**

All goods / services purchased via the purchase order system must be officially received prior to any accounts being paid. Once goods / services are delivered to CITG, it is the IT Manager’s responsibility to officially receive them. This is done by marking a copy of the purchase order “Received”, along with the date of receipt and the signature of the person receiving the goods / services. This document, along with any invoices is to be passed on to the CITG Treasurer.
Chapter 4 Computer Software

1. Software Policies

4.1. Software Policies

College software must adapt to users needs for useful information and functionality. This software should model the Colleges in their changing and complex operations. Creating or buying software is much more than a question of resources and cost. It can also be a question of remaining efficient, and compatible with other agencies. There is a need on the policy level to provide some sort of direction for software development, purchase and maintenance.

4.1.1. Proprietorship of Computer Software

All software developed during work hours by personnel paid by the hour is the exclusive property of CITG.

Additional programs and software policies apply to:

1. Purchased Software
   Purchased software and software documentation may be copied as specified by the vendor licence agreements. No versions of any purchased software are permitted beyond the number that Colleges have purchased. This applies to all organisational personnel.

2. Unauthorised software
   Personnel may not purchase or write their own software for use on College computers without authorisation. They may not bring to Colleges any software in any form that is not either the property of or licensed for use by either CITG or the College. The downloading of any unauthorised software to College hardware away from any College site is also not permitted. Any violation of this policy subjects the offender to immediate disciplinary action at the discretion of the College Principal and/or the reimbursement of all costs associated with such action.

2. Purchasing Software

4.2. Purchasing Software

The decision to purchase software is arrived at when in-house development cost is prohibitive or when there is a lack of programming talent available in the time frame required for its development. Also, it is totally impractical to write software that is already available as an “off-the-shelf, shrink wrapped” package.

When software cannot be programmed “in-house” it will have to be obtained in one form or other. If a shrink-wrapped program is not available, it may be necessary to contract outside software contractors using the CITG purchasing policies.

4.2.1. Procedure for CITG Software Purchasing

CITG purchased software is requisitioned against the CITG budget for software. The IT Manager or the CITG Chairman must sign all orders against the CITG budget.
1. Requesting CITG to purchase software.
Any College may request CITG to purchase software relevant to all member Colleges. Software used exclusively by one College is to be purchased by that College.

The request for new software is to be made using the standard “CITG Request Procedure” as defined in this manual. The requestor should provide as much relevant detail as possible, including where available:
   a. Software title
   b. Supplier contact details
   c. Machine/s software is to be loaded on
   d. Approximate costs (or quotations)
   e. Purchase rationale / benefits

2. Approval
The IT Manager is to evaluate the software as per the software evaluation procedure and make recommendation to the CITG Committee. Based on this information, the CITG Committee can approve or disapprove the request, note the decision on the request form, providing explanation for the decision where necessary. If the requestor is not satisfied with the decision/explanation, they may appeal to the committee.

4.2.2. Other Software Requisition Procedures
Colleges may of course purchase software specific to their individual needs, utilising their own purchasing procedures. CITG must be contacted prior to purchase to ensure that the new software is compatible with existing College systems. CITG reserves the right to remove any such software, or to refuse assistance, including the Help desk, for any software that has not been checked.

4.2.3. Contract Programming
To be written.

4.2.4. Evaluation of Packaged Software
There are major issues to be addressed when purchasing packaged software that can apply to almost any type of software supplier. They are:
- Will the vendor be in business next year?
- What warranty/support will be provided?
- Will the software integrate with other software used by Colleges?
- What flexibility will the software package provide?
- Is the current College hardware compatible with the proposed software?
- What type of training is offered?
- Is the documentation user friendly?
- What other expenses may be involved (data conversion etc.)?
- Can the vendor provide modifications to the software?
- Is there an upgrade planned in the near future?
- Is there a vendor Help Desk?
- What is the vendor’s reputation?
- How many users currently use the software?
- Will the vendor supply the names of current users?
To discover how difficult or easy it will be to implement the proposed software the following issues should be addressed:

- How complex is the installation procedure?
- Will the vendor provide installation assistance?
- How easy is the software to maintain?

To evaluate vendor-supplied software, ask current or former users the following:

- Would they buy from the same vendor again?
- Did the software perform as promised?
- Was the training of value?
- Was the documentation easy to follow and complete?
- Were there any implementation problems?
- Did the installation or operation have any hidden costs?
- Would the referenced user allow a visit to their site to see how the software is working and talk to operations personnel?

New packaged software must be evaluated, whether for new applications or for placement on the “approved software list,” especially if this purchase will commit Colleges to buy in volume. This evaluation will take the form of a feasibility study as defined in this manual. The extent of this study/evaluation will depend on the cost/impact of the proposed software. Depending on the type of software considered, use the following procedures:

1. General Use software evaluation
   A person or formal committee will be responsible for general use packaged software evaluation. A request for such evaluation can come from a user or from CITG. ITS002 is a work sheet used for software evaluation.

   Wherever possible, more than one vendor should be evaluated for the same kind for software. Computer publications, as well as their advertisements, are a good source of evaluation information.

2. Client/server and vertical software evaluation
   Client/server and vertical packaged software will require a preliminary operations hand-on test followed by controlled client/server or workgroup prototype operations testing. A users’ evaluation will also be required. The amount of time required for each controlled test will vary with the complexity of the software operation and the number of planned future users. That is, the more users, the safer the software should be.
Software Evaluation Worksheet

Software Title: ___________________________ Version: _______________________
Software Description: _________________________________________________________
Vendor: ___________________________ Address: _______________________
Contact Person: _________________________ Phone #: _______________________
Tested by: ___________________________ Date: __/__/__
Machine software tested on: ________________ Date: __/__/__
Software copied to other machines: ______________________________________________
___________________________________________________________________________

Approved/Disapproved By ____________________________ Date ___/___/___

Comments
Chapter 5  IT Equipment

1. IT Equipment Policies

5.1. Equipment Policies

College’s IT equipment must adapt to users needs for functionality. This equipment should model Colleges in its changing and complex operations. Leasing or buying equipment is much more than a question of resources and cost. It can also be a question of remaining efficient, and compatible with other agencies. There is a need on the policy level to provide some sort of direction for equipment purchase and maintenance.

5.1.1. Use of IT Equipment

IT equipment is intended for use by College employees to provide operational support for their job tasks. It is the responsibility of CITG to ensure that staff have the necessary equipment required to perform their jobs accurately and efficiently. It is the responsibility of College staff to ensure that the equipment is not misused.

Misuse of IT equipment includes but is NOT limited to:

1. Unauthorised equipment
   Personnel may not purchase or install hardware for use on College networks without authorisation. They may not bring to College any hardware in any form that is not the property of their respective College, or leased by the College.

2. Utilising equipment for private purposes and in contravention of the intended purpose it was provided for.

3. Destruction of, or damage to equipment, belonging to a member College or other clients.

4. Intentional unauthorised copying of copyright protected material or infringement of license agreements and other contracts;

5. Violation or attempted violation of any computer network’s security system;

Any violation of this policy subjects the offender to immediate disciplinary action at the discretion of the College Principal. Additionally, illegal acts involving the use of equipment may be subject to prosecution by local, state or federal authorities.

5.1.2. Equipment Warranties

In most cases, the ongoing maintenance costs of equipment can far exceed the original cost of that equipment. In the IT industry, this is often referred to as the TCO or “Total Cost of Ownership”. One means of reducing TCO is through the use of comprehensive equipment warranties, thus reducing the maintenance costs of the equipment. Wherever possible, the following warranty conditions should be part of any IT equipment purchase:

1. For desktop equipment, a three-year next-day on-site warranty covering all parts and labour.

2. For minor peripheral equipment, a twelve month, RTB (return to base) warranty.
3. For major equipment such as servers and networking infrastructure, a comprehensive three-year on-site warranty with the capacity to extend this into an ongoing on-site maintenance contract.

2. **Purchasing Hardware**

5.2. Purchasing Hardware

The decision to purchase equipment is arrived at when existing equipment is unable to perform the tasks required by the users. This would occur due to; existing equipment no longer capable of completing the tasks required, either by fault or age or a change in the tasks being performed by the users.

5.2.1. **Procedure for CITG Equipment Purchasing**

CITG purchased equipment is requisitioned against the CITG. The IT Manager or the Chairman of the CITG Committee must sign all orders against the CITG budget.

1. Requesting CITG to purchase Hardware.
   
   Any College may request the IT Department to purchase equipment relevant to all member Colleges. Equipment used exclusively by one College is to be purchased by that College.
   
   The request for new equipment is to be made using the standard “CITG Request Procedure” as defined in this manual. The requestor should provide as much relevant detail as possible, including where available:
   
   - Equipment type (make and model if possible)
   - Supplier contact details
   - Approximate costs (or quotations)
   - Purchase rationale / benefits
   - Proposed location of equipment

2. Approval
   
   The IT Manager is to evaluate the equipment as per the equipment evaluation procedure and make recommendation to the CITG Committee. Based on this information, the CITG Committee can approve or disapprove the request, note the decision on the request form, providing explanation for the decision where necessary. If the requestor is not satisfied with the decision/explanation, they may appeal to the committee.

5.2.2. **Other Equipment Requisition Procedures**

Colleges may of course purchase equipment specific to their individual needs, utilising their own purchasing procedures. CITG must be contacted prior to purchase to ensure that the new equipment is compatible with existing College systems. CITG reserves the right to disconnect any such equipment from the CITG network, or to refuse assistance, including the Help desk, for any equipment that has not been checked.
5.2.3. Evaluation of New Equipment

There are major issues to be addressed when purchasing equipment that can apply to almost any type of supplier. They are:

- Will the vendor be in business next year?
- What warranty/support will be provided?
- Will the equipment integrate with other equipment used by CITG?
- What type of training is offered?
- Is the documentation user friendly?
- Is there a vendor Help Desk?
- What is the vendor’s reputation?
- How many users currently use the equipment?
- Will the vendor supply the names of current users?

To discover how difficult or easy it will be to implement the proposed equipment the following issues should be addressed:

- How complex is the installation procedure?
- Will the vendor provide installation assistance?
- How easy is the equipment to maintain?

To evaluate vendor-supplied equipment, ask current or former users the following:

- Would they buy from the same vendor again?
- Did the equipment perform as promised?
- Was the training of value?
- Was the documentation easy to follow and complete?
- Were there any implementation problems?
- Did the installation or operation have any hidden costs?

Major purchases (greater than $10,000) of equipment must be evaluated, whether for new applications or for replacement, especially if this purchase will commit Colleges to buy in volume. This evaluation will take the form of a feasibility study as defined in this manual. The extent of this study/evaluation will depend on the cost/impact of the proposed equipment. Depending on the type of equipment considered, use the following procedures:

1. Mass use equipment evaluation
   A person or formal committee will be responsible for mass use equipment evaluation. A request for such evaluation can come from a user or from CITG. ITS005 is a work sheet used for equipment evaluation.

   Wherever possible, more than one vendor should be evaluated for the same kind for equipment. Computer publications, as well as their advertisements, are a good source of evaluation information.

2. Single use or infrastructure equipment
   Due to the technical nature of large or infrastructure equipment, wherever possible the end user in conjunction with a staff member from the IT Department should
evaluate it. ITS005 is a work sheet used for equipment evaluation.

<table>
<thead>
<tr>
<th>Equipment Evaluation Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref: ITS005</td>
</tr>
<tr>
<td>CITG</td>
</tr>
<tr>
<td>Ph: ext 777</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Equipment Type:</th>
<th>Make/Model:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td></td>
</tr>
<tr>
<td>Purpose:</td>
<td></td>
</tr>
<tr>
<td>Vendor:</td>
<td>Address:</td>
</tr>
<tr>
<td>Contact Person:</td>
<td>Phone #:</td>
</tr>
<tr>
<td>Tested by:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

**Evaluation Summary**

Attach extra pages, documents and test results.

<table>
<thead>
<tr>
<th>Approved/Disapproved By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.
Equipment Register (Proposal)

5.3. Equipment Register

As a measure of controlling CITG based equipment, an Equipment Register is to be maintained to assist in the allocation and retrieval of all Equipment. The register also ensures that there is no confusion as to who has borrowed the equipment and keeps an accurate history of a particular piece of equipment and the purpose for which it has been used. This excludes equipment belonging to, or maintained by individual member colleges.

4.3.1. Procedure for IT Equipment Register

All equipment must be booked and registered prior to its removal from the CITG office or storeroom. This is to ensure that the IT Manager is aware of all equipment bookings and can approve the use of equipment before it is loaned out.

1. Booking equipment.

All IT equipment bookings must be authorised by the IT Manager. A booking is made through the CITG Help Desk. The booking request must include a description of what the equipment will be used for and the duration for which it will be needed. The timings need to be closely adhered to in order for the booking system to be successful, as multiple bookings for a single piece of equipment may exist in the same day.

3. Registering Equipment.

The Equipment Register MUST be filled out in full and signed by the person borrowing the equipment before it can be removed from the CITG office or storeroom. The register must also be signed upon the equipment’s return. Only the CITG Staff can sign for the return of equipment. This is designed to cover the person who last borrowed the equipment in the case of the particular item being misplaced or stolen at a later date. Refer to Equipment Loan Register.
## Equipment Loan Register

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Phone No.</th>
<th>Camera</th>
<th>Ltd</th>
<th>Radio</th>
<th>Net</th>
<th>Cd-Rom</th>
<th>Projector</th>
<th>Other</th>
<th>Details</th>
<th>Return Date</th>
<th>Signature</th>
<th>Rtn</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6 Use of Systems

1. E-mail Policy

6.1. E-mail Policy

This section sets down the policies used to govern the use of staff E-Mail facilities provided by CITG. It is applicable to all Staff of CITG member colleges or people acting as agents for these colleges and to all e-mails originating from the CITG network, regardless of purpose or destination.

6.1.1. Acceptable Use

E-Mail facilities are provided for use by College staff, and by agents as declared by College Heads on the basis that it is used within the following guidelines.

Staff shall not;

- Transmit material which may be considered offensive or contravenes the College's Sexual Harassment or Equal Employment Opportunity policies.
- Transmit material which is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Transmit material, software or other information protected by copyright laws.
- Represent personal opinions as those of the College
- Reveal or publicise confidential proprietary information, for example, financial information, student information, marketing strategies and plans.
- Engage in sustained high volume network traffic not related to work, for example, transmission of e-mails containing large graphics, video and sound content.
- Transmit messages using another person’s user name or network account

6.1.2. E-mail Storage

All copies of e-mails that are inappropriate for storage on the CITG e-mail system should be deleted immediately. All other e-mails must be archived as soon as practical. Copying e-mails to subject matter folders can facilitate better management of large volumes of e-mails.

6.1.3. Non-Compliance

The respective College will review any alleged breach of this Acceptable Use Policy on an individual basis. If the alleged breach is of a very serious nature which breaches the employee's duty of fidelity to the college (for example, emailing confidential information of a resident), the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of the company the breach may be treated as grounds for dismissal.

Otherwise, an alleged breach shall be dealt with as follows:
• Initially, the employee shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, be asked to desist from or where applicable to remedy the breach.

• If the breach is not desisted from or remedied, the College may either withdraw the employee's access to the Internet or provide a first warning to the employee, to which the employee shall have an opportunity to respond.

• If the infringing conduct continues the employee may be given a second and a third warning, to each of which he or she shall have an opportunity to respond.

• If a breach is committed after the third warning the employee may be dismissed.

2. Internet Access Policy

6.2. Internet Access Policy

This policy sets out guidelines for acceptable use of the Internet by employees of CITG and its’ member colleges. The primary purpose for which access to the Internet is provided by CITG to college employees is to assist them in carrying out the duties of their employment. They may also use the Internet for reasonable private purposes which are consistent with this Acceptable Use Policy. They may not use the Internet access provided by CITG in such a way as to significantly interfere with the duties of their employment or to expose Widgets Ltd to significant cost or risk of liability.

6.2.1. What is Acceptable Use

Subject to the balance of this policy, employees may use the Internet access provided by CITG for:

• Work-related purposes;
• Using instant messaging software for personal purposes;
• Accessing the World Wide Web for personal purposes; and
• Utilising any other Internet service or protocol for personal purposes after obtaining permission to do so from the head of the relevant college;

provided in each case that the personal use is moderate in time, does not incur significant cost for CITG / College and does not interfere with the employment duties of the employee or his or her colleagues.

6.2.2. What is not Acceptable Use

Except in the course of an employee's duties or with the express permission of CITG / the College, the Internet access provided by the CITG may not be used for:

• personal commercial purposes;
• sending unsolicited bulk email;
• disseminating confidential information regarding CITG / the College;
• any illegal purpose;
• knowingly causing interference with or disruption to any network, information service, equipment or any user thereof;
• disseminating personal contact information of officers or employees of CITG / theCollege without their consent;
• knowingly causing any other person to view content which could render the company liable pursuant to equal opportunity or sex discrimination legislation at the suit of that person; or
• knowingly downloading or requesting software or media files or data streams that the employee has reason to believe will use a greater amount of network bandwidth than is appropriate.

6.2.3. Non Compliance
The respective College will review any alleged breach of this Acceptable Use Policy on an individual basis. If the alleged breach is of a very serious nature which breaches the employee's duty of fidelity to the college (for example, emailing confidential information of a resident), the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of the company the breach may be treated as grounds for dismissal.

Otherwise, an alleged breach shall be dealt with as follows:

• Initially, the employee shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, be asked to desist from or where applicable to remedy the breach.
• If the breach is not desisted from or remedied, the College may either withdraw the employee's access to the Internet or provide a first warning to the employee, to which the employee shall have an opportunity to respond.
• If the infringing conduct continues the employee may be given a second and a third warning, to each of which he or she shall have an opportunity to respond.
• If a breach is committed after the third warning the employee may be dismissed.

3. Network Access/Sharing Policy

6.3. Network Access/Sharing Policy
The ResNet policy has been established to provide a set of rules and guidelines for the proper and responsible use of the CITG/College computing and network resources, effective protection of individual users, equitable access, and proper management of these resources. These guidelines are intended to supplement, not replace existing laws, regulations, agreements, policies, and contracts, which currently apply to these services.
Although the peer-to-peer file sharing is not prohibited, it can be used for the illegal downloading and distribution of audio, video, software and other files. Downloading or distributing material without permission of the copyright holder is a violation of federal and state law, even if it is not for profit. The penalties can be significant, including imprisonment and fines. Our refusal to censor access in no way condones violations of copyright or intellectual property laws.

Copies of this Policy will remain available via ResNet's web site.

6.3.1. **Acceptable Use**

Users of ResNet are bound by the University of Queensland Internet Code of Practice Policy. This policy can currently be found at:


ResNet users are additionally bound by the following rules and regulations intended to preserve the integrity and accessibility of all computing resources:

1. Residential Computing network services and wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware and in-room data points.

2. College data points may not be used to provide network access to anyone other than the resident assigned to the data point. Residents will be held responsible for all packets generated by their assigned connection.

3. Servers of any kind are prohibited without written authorisation from CITG. Individuals may use only the IP address assigned to them by CITG. Unauthorized use of a "fixed" IP address is prohibited.

4. The residential network is a shared resource. Network uses or applications, which inhibit or interfere with the use of the network by others, are not permitted. Examples include but are not limited to file-sharing applications such as network game servers, and any excessive consumption of bandwidth.

5. The residential network may only be used for legal purposes and to access only those systems, software and data for which the user is authorised. Sharing access to copyrighted material (including MP3 files from copyrighted music media and digitized video from copyrighted motion pictures, etc.) on the network is prohibited.

6. Respecting the rights of other users, including their rights as set forth in other University policies for students, faculty, and staff, is required at all times on the network. These rights include but are not limited to privacy, freedom from harassment, and freedom of expression.

7. Users are required to know and obey the specific policies established for the systems and networks they access.

8. The residential network is provided for uses consistent with the academic mission of the institution. The network may not be used for commercial purposes nor for unsolicited advertising. Users may not provide open access to files/folders on their computers which contain anything that is protected by copyright (this includes MP3 files from copyrighted music media and digitized video from copyrighted motion pictures, etc.), or
which would be in violation of the University's and/or community standards.

9. Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited. Prosecution under State and Federal laws may also apply. This includes the use of an IP address not specifically assigned to the individual using it and the use of a forged or false identity.

10. Any activity that can be deemed hostile such as port scans, email-bombs, ping-bombs, etc. are prohibited.

6.3.2. Malicious Attacks

Malicious attacks, are considered the most grievous breach of the acceptable use policy, and will be dealt with accordingly. If it is proved that a user has executed a malicious attack on CITG systems or another user, then they shall be dealt with the full extent of college disciplinary measures as per “Non-Compliance below”.

Malicious attacks can be defined as, but not limited to the following;

- Denial of service attacks on another machine
- Hijacking another machines network address
- Loaded unsolicited material on another users machine, including “porn chops”
- Deliberately attempting to compromise the security of another machine
- Hijacking or attempting to hijack another users network identity.

If a resident believes they are the victim of a malicious attack, particularly where pornographic materials are involved, they should follow the following steps;

1. Shut down your machine and remove it from the network immediately.
   (disconnect the network cable)
2. Contact the CITG help desk (777) and report the problem.
3. Contact the college office and report the attack.

The college in conjunction with CITG will investigate the attack. This will include an inspection of the machine that has been compromised. Hence it is important that the machine not be altered until CITG staff have completed this inspection. It should be noted that this inspection will take a very high priority so as to minimise the inconvenience to the resident. Where appropriate, CITG staff will assist the resident with the removal of unsolicited files from their machine.

6.3.3. Non-Compliance

Use of ResNet constitutes FULL agreement and understanding of this Acceptable Use Policy and any future modifications there to. Violations of this policy may result in termination of connection, disciplinary sanctions, as well as legal sanctions. CITG Administrators have authority to control or refuse access to the network to anyone who violates these policies or who threatens the rights of other users. Administrators have the authority to suspend network access without notice for a user/computer that
is believed to have been the source of an alleged violation pending investigation of the violation and satisfactory resolution of the complaint.

All complaints / infringements will be reported to the relevant college head who will institute their own disciplinary actions. An alleged breach shall be dealt with as follows:

- Initially, the resident shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, a mandatory two week suspension from all CITG / College based computer facilities will be imposed.

- If when computing privileges are reinstated, the breach is not desisted from or remedied, the College may either permanently withdraw the resident’s access to the computing facilities, or require the resident to show cause as to why they should be allowed continued residence.

- If the infringing conduct consists of a major breach of the University’s Policies, then the College is also obliged to inform the relevant University authority

6.3.4. Underage Access

Legislation by the Federal Government restricts Internet services for people under 18 years of age. As colleges contain residents under the age of 18, this legislation is relevant to the use of the Colleges’ network, and more specifically to the use of the pay-as-you-go Internet access. This legislation prohibits CITG from giving full Internet access to people under the age of 18 without written permission by a parent or guardian. Details of this legislation are available at the Australian Broadcasting Authority website.

To fulfill this requirement, all residents under the age of 18 who require access to College computing facilities must complete the “CITG Under 18 Access Permission” form.
**Under 18 Access Permission**

**DIRECTIONS:**
Please complete the details below and return to the administration office of your college.

<table>
<thead>
<tr>
<th>Student Name:</th>
<th>Student Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

I give permission for the above student for whom I am the parent/guardian, to have full access to the internet via the College Computer network. I agree that the College will not be held responsible for any content seen by the student.

<table>
<thead>
<tr>
<th>Name of Parent/Guardian:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7  IT Department Operations

1. IT Department Operations Policies

7.1. IT Department Operations Policies

This section sets down the policies used to govern CITG’s day-to-day operations. The IT Systems are restricted to College and identified vendor personnel; but because of today’s distributed networks, access is not limited to persons physically entering College premises. They can also be accessed through telecommunications and every precaution needs to be taken.

7.1.1. Staffing of CITG

Wherever possible, there is to be a CITG staff member in the CITG office at all times during nominated CITG work hours. If circumstances prevent this, it is essential that the telephones in the department be diverted to message bank, and that the messages are responded to within one hour of returning to the office. Where appropriate, telephones may be diverted to a mobile telephone.

7.1.2. Computer Room Security and Safety

To maintain proper computer room security and safety, the following policies are to be adhered to:

- Restricted access
  No person may enter the CITG office without the accompaniment of a CITG staff member, or the Chairman of the CITG Committee.
- Power supply
  The computer room must have a separate power circuit connected to the main power source for the building. A UPS or fail safe device is required to prevent hardware damage and data loss if the main power fails. A generator should be available to provide emergency power in the case of extended power failure.
- Air Conditioning
  The Computer room must have it’s own air conditioning system.
- Fire precautions
  Fire extinguishers of the appropriate type for electrical fires must be available as near as possible to the computer room.
- Data backup
  Database and file backups will be kept as current as is reasonable. Off-site data and software backups will be maintained.

7.1.3. Housekeeping

Following are policies that apply to housekeeping in the computer room.

- No smoking, eating or drinking is permitted.
- CITG Personnel are responsible for maintaining a clean working area.
- The computer room is not to be used for anything other than assigned operations.
- Temperature and air-flow are to be monitored and kept within recommended ranges for the equipment.
7.1.4. Tape storage policies

The limited life span of magnetic tapes and their susceptibility to external interference such as excessive heat, moisture and magnetic fields mandates the close monitoring of their condition and storage location. On-site storage of tapes should be a fire rated safe positioned in a cool dry area. Off-site backup storage should conform to the same standards.

2. General Operations

7.2. General Operations

This section covers general procedures to be followed by CITG personnel and by any visitors.

7.2.1. Security and Safety

- The computer room is to be kept locked at all times
- The CITG Office is to be locked whenever IT personnel are not in attendance.
- Access to CITG is restricted to CITG personnel, or those accompanied by CITG personnel. In an emergency situation, the CITG Committee Chairman, or delegated officer, may provide permission for another staff member to gain access. This access is to be documented in memo form, detailing the reasons behind the access and bearing the signature of the authorising officer.
- Fire extinguishers and/or their controls are to be easily identifiable. Instructions for use must be posted on or near the instruments.
- Operations personnel are responsible for knowing:
  a. Location of Fire equipment and their operation.
  b. Emergency power off procedures.

7.2.2. Safety

- Eating, drinking and/or smoking are not permitted in the computer room. Signs to this effect are to be posted in the computer room and on or near the entrance.
- CITG personnel who are under the influence of prescribed sedatives or similar medication are to be given assignments that will not endanger the operator or the equipment.
- CITG personnel are responsible for the general cleanliness in their areas. Items removed for use (including disks) should be returned as soon as applicable.

7.2.3. Downtime procedures

Where there are hardware or software failures, downtime procedures require CITG personnel to describe and record certain information in an Incident and downtime log. A copy of the log sheet has been included as Exhibit 4-1. The log should contain:

- The Date and time of the incident.
- A brief description of the incident.
- Which systems were affected by the incident.
- Actual time system was affected (downtime).
• Where an incident is regarded as significant (ie. Not just a simple reboot or lockup), it is to be recorded in the “IT Help Desk” system. A printout of the incident from the system is to be placed in the log detailing:
  a. General conditions at the time of failure
  b. Detailed explanation of fault
  c. Any and all corrective action taken to rectify the fault and the results.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Incident Type</th>
<th>Issue #</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total downtime for period

* All major incidents must have a corresponding entry in help desk system (issue #), copy in rear of folder.

Exhibit 4-1

7.2.4. **Disk/CD Handling**

Proper disk handling ensures data availability for jobs and reduces read-write errors. This applies both to floppy disks and compact discs.

• Disks/CDs are to be stored in proper containers when not in drives.
• Clean hands are a must for personnel handling disks/CDs.
• Disk/CD storage containers are to be filed in place when not in use.
• Contents of disks and CD-Rs (CD Recordable) are to be identified by external labels placed on the front of the disk/CDR

7.2.5. **Tape Handling**

• Clean hands are a must for personnel handling tapes.
• Tape drives should be cleaned in accordance with the manufacturers recommendations. Drive cleaning should be recorded in the backup log.
• Tapes are to be kept in protective containers when not in use.
• Long term storage for data tapes is to be in a fire rated safe.
3. Operating Procedures

7.3. Operating Procedures

CITG operating procedures relate to tasks specifically performed by CITG personnel and are generally the result of the Operations Policies.

7.3.1. Daily Operations Procedures

The heart of the IT Systems is the computer network. Operation of the network is the duty and responsibility of CITG. In order for the system to operate efficiently and effectively, a number of daily tasks need to be performed. These operations should be checked off on ITS003, the “CITG Daily Checklist”. The checklists are to be kept in a folder for reference.

It is the responsibility of the IT Manager or delegate to check that all operations on the checklist have been checked off and the form signed off prior to departing for the day.

ITS003 (To be developed)

7.3.2. Data Backup Procedure

To ensure the safe retention of Council data, it is necessary to perform backups on all essential College systems on a daily basis. The IT Manager is responsible for determining what components of the IS System require backing up. A detail of what information is being backed up is to be kept at the front of the Backup log folder. A copy of this information is also to be stored with this manual.

1. Backup Device
   There is a single “network” tape backup system in use in CITG. These tapes are to be rotated so as to make efficient use of the tapes at hand. CITG uses the “Grandfather, Father, Son” method of tape rotation. This method uses a four-week cycle based on:
   a. A daily tape for Monday through Thursday used every week. (Son)
   b. A weekly tape for the first three Fridays of the cycle. (Father)
   c. The forth Friday tape from each cycle is kept as a monthly tape. These are kept aside for 1 year or 13 cycles. (Grandfather)

2. Verification
   The backup software for each system backup device is to perform a verification routine to ensure that the data backed up is correct, and that a usable backup has been created.

3. Backup Log
   A daily log of all backups, successful or not is to be kept for all systems. An example of this log has been included as Exhibit 4-2. This log should take the form of one page per backup cycle and record:
   a. Backup Day/Date.
   b. Device being backed up.
   c. Tape number used for backup.
   d. Success/failure of backup.
   e. When tape drive cleaning has been done.
   f. Signature of officer completing the log.

Exhibit 4-2 (to be developed)
7.3.3. **Off-site Backup Procedures**

To ensure data security in the event of disaster, the “Grandfather” tapes as described above are to be kept in a secure location outside of CITG premises. The most efficient method of doing this is to utilise a storage facility at a CITG member College other than that where the computer system is located.

The tapes should be taken to the Off-site location the Tuesday following the successful backup, and their removal recorded on the backup log. If for some reason the backup monthly backup fails, the next successful backup is to be used, and the tapes replaced from stock.

---

## 4. IT Technical Support

### 7.4. IT Technical Support

CITG provides technical support for all systems under its control. Technical support is monitored and recorded using a help desk system. This system is maintained by CITG staff.

#### 7.4.1. **IT Maintenance Procedure**

Users are able to log requests with the IT Department one of three ways.

- On-line “Task Request Sheet”
- Complete ITS004 “Information Technology Task Request Sheet”
- Telephone (used primarily for urgent requests or to seek advice)

1. **Priorities**

   Assistance is provided to users based on a priority system, based on the type of request, and what if any are the effects of not completing the request. The five priorities are:

   a. **Critical**
      
      Staff unable to operate due to fault
   
   b. **Severe**
      
      Staff Operation severely hampered
      Multiple residents operation hampered
   
   c. **Minor**
      
      Staff operation hampered / minor training,
      Individual resident fault
   
   d. **Enhancement**
      
      System enhancement (eg. new equipment, shifting equipment)
   
   e. **Review**
      
      Management Review (strategic operation)

2. **User Responsibilities**

   a. Logging the request with CITG
   
   b. Providing adequate information to enable repair, including details of:
      
      **Staff Fault:**
      
      i. Equipment
      ii. Location / Telephone
      iii. Details of fault / request
   
      **Resident Fault:**
      
      i. Name
      ii. Student Number (8 digits)
      iii. Telephone ext
iv. College
v. Detailed description of problem
c. Checking the resolution for accuracy
d. Prioritising work into critical (telephone request), severe-review (written request). Some rating 2 & 3 jobs may be handled by telephone request, such as minor program faults, questions. However if the IT officer called is not able to respond, a written request will be required.

3. CITG is responsible for
   a. Ensuring all requests are entered onto the database
   b. Prioritising requests into ratings as per definition
   c. Responding to critical calls as soon as possible upon receipt
   d. Resolving requests according to priorities from the maintenance list
   e. Updating the database with progress
   f. Providing feedback to the client on progress of request

7.4.2. Procedure
IT Repairs

Start

Is Request a purchase

Is request equipment fault

Can repair be completed in-house

Yes

Perform Installation / repair

Yes

Ensure Installation and configuration correct

No

Perform tests to ensure correct operation

Does equipment work correctly

Yes

End

No

Send equipment to appropriate supplier

Are external supplies required

Yes

Obtain quote for repair

Is equipment under warranty

Yes

Accept quote for repair

No

Adviser supplier to complete repair

Does item require replacement

Yes

Request that supplier return unrepaired item

No

Yes

No

No

Yes

No
### Information Technology Task Request Sheet

<table>
<thead>
<tr>
<th>Name __________________________</th>
<th>Equipment Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username _________________________</td>
<td>Type: ______________</td>
</tr>
<tr>
<td>Location ____________ Date <strong><strong>/</strong></strong>/____</td>
<td>Label / Model: _____________________</td>
</tr>
<tr>
<td>Dept ____________ Ph: __________</td>
<td>Location: _____________________</td>
</tr>
</tbody>
</table>

#### Equipment Details

**Type:** _____________________  
**Label / Model:** _____________________  

**Location:** _____________________

#### Request Type

- [ ] Security  
- [ ] Training  
- [ ] Fault Report  
- [ ] Purchase Required  
- [ ] Software  
- [ ] Hardware  
- [ ] Network  
- [ ] Telephones

#### Request Description

Please provide a detailed description of the request, including:
- exact error message, and what you were doing at the time
- note if a recurrent problem
- requisition and technical specifications of required purchase
- contact name and number if supplier known

Any actions taken by you to resolve this:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
Chapter 8 IT System Security

1. IT Systems Security Policy

8.1. IT Systems Security Policy

This section sets down policies used to ensure data security throughout the College’s computer systems. They take into consideration both physical and electronic access to College systems.

This section covers procedures to insure data security throughout the computer system. These procedures are designed to ensure that the management and systems operations audit policies will be satisfied and to support their enforcement.

8.1.1. Data Security Responsibility

Responsibility for the security of College IT Systems is delegated by the CITG Committee to the IT Manager. It is their responsibility to ensure that all security policies and procedures are adhered to.

The IT manager may only grant security access to a specific College’s files, or alter the access of personnel within a College if permission has been given in writing by that College Manager/Bursar. It is the responsibility of College Manager/Bursar to ensure that individual staff have the security access required to perform their duties. It is also the responsibility of College Manager/Bursar to ensure that no other policies or laws are violated by the security privileges granted to a user (eg finance policy).

8.1.2. Physical Security

The basis of all data security should be the physical security of the machines that access the data. It is the responsibility of College managers/Bursars and all employees within the college to ensure that all workstations and terminals used to access College systems that are not deemed student/public access terminals, are secured from public access.

Where a terminal is vulnerable to unauthorised public access, it is the responsibility of the user to ensure that the machine is not logged in to any College system during any period when the terminal is unattended.

8.1.3. Firewall

CITG is to maintain a firewall system to protect College’s data from unauthorised access. It is the IT Managers responsibility to ensure that the firewall system is operational and correctly configured. Any breaches of the firewall should be reported to the Chairman of CITG as soon as possible.

8.1.4. User Accounts / Passwords

User accounts are only to be provided to College staff, students contractors or those specifically authorised by the College Manager/Bursar. Passwords for all College systems are to be at least six (6) characters long, and have an expiry date no longer than sixty (60) days.
Accounts and security levels for new staff/contractors must be verified and signed off by the relevant College Manager/Bursar.

**8.1.5. Virus Protection Policy**

CITG must at all times maintain a virus protection regime on the computer system. Due to the rapid deployment methods and constant mutation of computer viruses, it is essential that the system used be constantly updated to remain current. Specific monitoring should include;

1. Resident protection on all file servers.
2. Resident protection on all workstations
3. Regular scanning of files on servers and workstations
4. Scanning of all incoming email

**8.1.6. Violations of Security Policies/Procedures**

Any serious violation of security policies/procedures be they accidental or deliberate must be reported as soon as possible to the members of the CITG Committee. It is their responsibility to determine the need for any investigation. Deliberate violations of policy/procedure will incur disciplinary measures at the discretion of the relevant College Principal. Disciplinary measures may include reprimand, forfeiture of salary increment, dismissal or for students, expulsion.

Independent of whether the violation is an internal or external matter, where it is considered a criminal offence, the Police should be informed. The decision to involve the police must be determined by the relevant College Principal (or delegate).

**2. Staff Induction Procedure**

**8.2. Staff Induction Procedure**

This procedure is designed to ensure that new staff entering Colleges understand the basics of the computer network, and the policies which govern its use and misuse. This procedure is designed to work in conjunction with Human Resource procedures.

This procedure to be written

**3. Security Alteration Procedures**

**8.3. Security Alteration Procedures**

These procedures are designed to ensure that College systems respond to the changing roles and responsibilities of College staff, while maintaining a secure computing environment. It also includes procedures for new and departing staff, which are to work in conjunction with Human Resource procedures, particularly termination procedures.

**8.3.1. Addition of User**

Requests for new security profiles to be set up on College systems should be made using the “Change to Existing Security” procedure. Due to number of tasks that have to be completed to set up a new user on the system, please allow 1-2 business days for a new user to be set up. This should be done prior to the start date of the employee.
8.3.2. Change to Existing Security

Requests for alterations to security profiles must be made on the “Alterations to IT System Security” form (ITS006), signed by the relevant College Manager/Bursar and lodged with CITG.

1. User Responsibilities
   a. Logging the request on the correct form with CITG
   b. Providing adequate information to enable change, including details of:
      iv. Users name and login name
      v. Current level of security in area required
      vi. Details of new security required or username for security equivalence.
   c. Obtaining the relevant Manager/Bursar’s signature
   d. Checking the new security levels for accuracy

2. CITG responsibilities
   a. Ensuring all requests are entered onto the help desk database
   b. Implementing and testing required changes
   c. Providing feedback to the client on progress of request

8.3.3. Removal of User

It is the responsibility of the College Manager/Bursar to advise CITG whenever a user’s access needs to be terminated. This should be done as soon as possible to avoid unauthorised access by people no longer associated with the College.

To log a request for the removal of a user, follow the same procedure as “Change to Existing Security. Where termination is to be expedited, telephone the request through as soon as possible.

4. Vendor/Contractor Access Policy

8.4. Vendor/Contractor Access Policy

These policies are designed to ensure that specific College systems are made available to external vendors and contractors where necessary, while maintaining a secure computing environment.

8.4.1. Remote Access Policy

It may on occasion be necessary for software vendors to remotely access CITG or College systems through a remote access connection. It is the responsibility of CITG staff to ensure that the appropriate connection systems are in place to allow such access and that it is secured so as to prevent unauthorised access. Such access may only be granted by CITG staff, and only when requested by and with the authority of a College Principal or Manager/Bursar (or delegate). Where access is required to software systems, CITG shall provide a temporary user ID providing access to the specific systems required by the vendor/contractor.
8.4.2. Physical Access Policy (Local College Systems)

Where necessary, physical access to secure local college equipment may be provided to vendors by individual college staff based on three criteria;

- Authority for each such access is expressly given by the College Principal or Manager/Bursar (or delegate)
- CITG staff are informed of the details of such access prior to it taking place.
- It is the responsibility of the college staff to supervise the vendor’s access and to ensure that there is no breach of security.

8.4.3. Physical Access Policy (Centralised Systems)

Where it is deemed necessary by the IT Manager, physical access to centralised college systems (those located at CITG) may be given to a vendor or contractor. Where access is required to software systems, CITG shall create a temporary user ID providing access to the specific systems required by that vendor/contractor. The IT Manager is deemed responsible for ensuring that data security policies are upheld.

8.4.4. Provision of Central or Remote Access

Requests for access to secure centralised systems must be made by the College Principal or Manager/Bursar (or delegate) directly to the IT Manager (or Delegate), either by telephone, or in writing

1. User Responsibilities
   a. Logging the request with CITG IT Manager.
   b. Providing adequate information to enable change, including details of:
      i. Vendor name.
      ii. Details of contact person.
      iii. Type of access required.
      iv. Purpose of access.
   c. Checking systems after vendor has completed work to ensure correct operation of altered systems.

2. CITG responsibilities
   a. Ensuring requests are dealt with in a timely fashion
   b. Monitor the vendor/contractor so as to maintain security and systems integrity.
   c. Re-securing systems upon completion of work.
# Alteration to Information Technology System Security

**Ref:** ITS006  
**CITG**  
**Ph:** ext 777

**Office use Issue no:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Username (existing users)</th>
<th>College</th>
<th>Date req</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Type</th>
<th>College System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Existing users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New User</th>
<th>Change existing user</th>
<th>Remove User</th>
<th>StarNet</th>
<th>NT (College Network)</th>
</tr>
</thead>
</table>

**Access Required**

Please provide a detailed description of the request, including - where applicable:

- Specifically which files/folders/functions need to be accessed
- If the access required is identical to another user (equivalence)
- Basic reason for required access

<table>
<thead>
<tr>
<th>Approved by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Must be Manager/Bursarr or higher

<table>
<thead>
<tr>
<th>Completed by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 9  Disaster Recovery (To be addressed)

1. Disaster Recovery Policy

9.1. Disaster Recovery Policy

This section sets down policies used to ensure the prompt recovery of CITG’s IT systems in the event of a disaster. They are restricted to the IT Systems, and are designed to work in conjunction with a College-wide disaster recovery plan.

9.1.1. Disaster and Recovery Plans

A well-organised disaster plan will help ensure CITG’s continued operation in the event of such an emergency. Likewise, an effective recovery plan in the event of major computer hardware or software failure is a necessity. College’s operation is significantly hampered when without the IT Systems operating in some manner for more than a couple of hours.

9.1.2. Core business Facilities

In the event of a major disaster, it would not be possible to restore all of College’s IT facilities quickly. The purpose of the plan is to enable Colleges to continue providing essential services to the residents and to maintain business operations. Not all of Council’s IT facilities are required to fulfil this criteria, therefore it is necessary to identify what specific facilities are required for College’s to operate.

To be determined by colleges

9.1.3. Extent of Authority

The IT Manager is the authority for all council computer systems. He/she has the primary responsibility for ensuring the successful implementation of the recovery plan. In order to complete this he/she has total authority over the placement and use of all College IT equipment in the event of the disaster plan being invoked. This authority is granted by mandate from College’s Chief Principal.

The authority to invoke the disaster recovery plan is solely that of the College Principal, or whoever is acting in that role.

2. Disaster Recovery Procedures

9.2. IT Systems Disaster recovery Procedures

This section sets down procedures ensure the prompt recovery of Colleges’ IT systems in the event of a disaster. The procedures included are specifically to recover the IT systems required to operate Colleges’ core business and are meant to cover the first 24-48 hours following a disaster. These procedures are designed to work in conjunction with a College-wide disaster recovery plan that covers infrastructure (buildings, furniture, cabling etc.) Also included are strategies for the complete recovery of all CITG systems.
9.2.1. Levels of Disaster

Different levels of disaster will require different responses. For instance, a major fire that destroys the Administration building will require significantly more planning and recovery than an electrical fault that damages equipment in the computer room.

Based on this, we define four levels of disaster:

- Loss of single server
- Loss of computer room
- Loss of admin building
- Total loss of facilities

9.2.2. General Procedures / Information

9.2.3. Loss of Core Server

9.2.4. Loss of Computer Room

9.2.5. Loss of Building

9.2.6. Total Loss of Facilities