

University of New England Information Technology Directorate

Security Policy

Version Control:

Ex CAUDIT Draft 2, September 1997

Amended DB/ITD 22/1/98

Amended DB/ITD 27/2/98

Amended DB/ITD 20/1/00

1. Introduction

1.1 Aim of the policy

This document states the information technology security policy of the University. Information Technology (IT) as used here includes computer systems and associated devices, networks and communications facilities.

This policy states the conditions of use of the University's IT facilities, the rights and responsibilities of users and administrators and the methods used to implement the policy.

The aim of this policy is to ensure:

- the provision of uninterrupted IT services
- the integrity and validity of data
- an ability to recover effectively and efficiently from disruption
- the protection of all the University's IT assets including data, software and hardware

1.2 Scope of the Policy

This policy covers all areas of the University, all staff, all students and all other users of the University's IT facilities.

1.3 Risk assessment

Prior to adoption of this policy, and periodically afterwards, the University shall carry out an Information Technology systems security risk assessment. The aim of such an assessment is to estimate the University's potential vulnerability, to ensure that security measures being taken are sufficient to reduce the risk to acceptable levels and to estimate the costs associated with achieving an appropriate level of security.

The potential risks include:

- users with higher than necessary levels of access;
- terminals not logged off correctly;
- shared user-ids and passwords;
- errors;
- disaffected employees;
- lack of security awareness;
- unauthorised access;
- viruses;
- dial-in access.
- lack of control over changes made to systems and/or data.
- legal consequences of security breaches.
- fire
- water
- sabotage
- risks associated with Internet access
- public embarrassment

2. IT Security Procedures

2.1 Physical Security

Access to secure areas, including computer rooms and PABXs, shall be restricted to authorised staff through the use of passwords, locks or access-control devices.

Visitors to such areas shall be permitted only under the supervision of authorised Information Technology staff. Details of visitors including name, time in, time out, and reason for entry shall be recorded in a log.

During non-working hours, secure areas shall be protected against intrusion by appropriate access control, surveillance systems or by security staff.

2.2 Hardware

The effect of electrical power outages and fluctuations shall be protected against by the installation of an uninterrupted power supply (UPS) and surge protection devices wherever practical.

IT facilities shall be adequately protected against fire, water and physical damage.

2.3 Software

All material associated with any computer system, including software and printed materials, which is not in the public domain must be treated in accordance with any applicable copyright agreements and restrictions. Such material must be licensed (if required) in an appropriate manner and may be obtained only in a legal manner from a legal source.

Users will not use the facilities of any computer system for storing, accessing or otherwise using any material which in any way infringes the commonwealth Copyright Act, 1968.

2.4 Data Security

An appropriate regular back-up schedule shall be implemented to protect all data and software. A sufficient number of backups of all data and software shall be stored off-site to protect against major damage at one location.

The backup procedures shall be clearly defined, regularly tested and documented in the Disaster Recovery Plan

The use of a computer system supplies the user with information about the computer system, as well as information about the University. This information is essentially private to the University and, in some cases, essential for the user to know in order to carry out useful work. Therefore, a trust relationship exists between the user and the University. This section describes the nature of this relationship.

a) A user will not use any account or otherwise attempt to gain access to any information that he/she is not authorised to possess.

b) A user will not use a computer system, or otherwise attempt to access any file or device, to disclose information that he/she is not authorised to possess.

2.5 Communications

The University grants the user a local account. The user can make an outgoing network connection to access (or attempt to access) a remote account, only when

- 1 the user is the holder of the remote account, or
- 2 the provider of the remote computer system recognises the remote account as a public access account.

The user will access, or attempt to access, remote accounts in a manner that abides by the conditions of use of the remote computer system.

The restrictions on outgoing connections are:

- 1 the provider accepts the type of connection
- 2 only the provider may make a connection, using network management equipment, to a University computer system or network management device.

The University may impose any other restrictions on an outgoing connection from any system under that University's control.

A user will inform the University of any details known to the user regarding any violation of this policy.

2.6 Internet Security

- The Internet will be treated as a potentially hostile environment.
- Only a limited number of registered systems will have Internet access.
- Security on these systems will be tightly controlled.
- A firewall will be used on all such systems.
- All data packets and connection requests will be controlled by the firewall.
- Only explicitly permitted traffic is allowed through the firewall. All other traffic is rejected.
- All traffic passing through the firewall must be capable of being logged and audited.
- Packet filtering will be used with rules which keep the risk to a minimum.
- Where possible, access by outside users will be restricted.

2.7 Electronic Mail

The University provides electronic mail facilities to support its academic and administrative functions. Any use of the facilities which interferes with these activities is forbidden.

The following are also forbidden in the use of electronic mail:

Use for any purpose which is illegal under state or federal law.

Use of another's identity.

Concealment or misrepresentation of name or affiliations.

Alteration of source or destination address.

Use for unauthorised commercial or private business purposes.

Sending material which harasses, intimidates, abuses or offends others.

Any user of the electronic mail system whose actions violate this policy, may be subject to restriction or loss of electronic mail privileges as well as other disciplinary actions.

2.8 Privacy

Users of electronic mail are advised that the privacy and confidentiality of electronic mail cannot be guaranteed. While system administrators will not monitor the contents of electronic mail messages in normal circumstances, the University reserves the right to inspect, copy, store and disclose the contents of electronic mail messages at any time. However, it will only do so when appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities. A system administrator who believes such action is necessary must first obtain the approval of the Deputy Vice Chancellor - Information Services (PVC-IS), or the head of the academic or administrative unit.

3. Users

3.1 Rights

Users have a right to privacy while engaged in legitimate activity. This right may on occasion be superseded as indicated in 3.3 below (Privacy). Users also have a right to adequate IT resources to carry out legitimate activity.

3.2 Responsibilities

Users' responsibilities include:

- being aware of all IT policies
- ensuring that confidentiality and privacy of data is maintained.
- the safekeeping of their user-id and password.
- ensuring the security of their terminal by logging off or locking it when it is left unattended.
- ensuring the security and privacy of print-outs produced from University computer systems.
- compliance with all relevant State, Federal and International law
- compliance with the provisions of this policy and all other University policies & procedures
- avoiding excessive use of IT resources, which may conflict with the rights of others

- compliance with any quotas or limits imposed by the University
- adherence to accepted community standards of expression or 'netiquette', when communicating with other people using any computer system.

Users will not harass or cause annoyance to other users by direct or indirect communication.

Users are subject to University Statutes, and State and Federal Laws, in regard to the content of any communication with other people made using any computer system.

Users will not forge electronic mail messages, news articles, or any other type of electronic correspondence.

Users will use their accurate and real identity, and identify, where appropriate, their positions in the University.

3.3 Privacy

Users have a legitimate expectation to privacy in the carrying out of approved activity. However, the University also has a legitimate right to inspect any data on a computer system (regardless of data ownership), to prevent, detect or minimise unacceptable behaviour on that computer system. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved. This section formalises this agreement.

- a) The University may monitor or use any account, device, or terminal without notice.

The University may inspect, without notice, any data on any resource

- b) owned by the University (regardless of data ownership), including electronic mail and other forms of communication.

In the course of carrying out computer system auditing operations, the University may access and copy any file on any computer system

- c) owned by the University. Subject to all other conditions of this policy, the University is obliged to maintain confidentiality as a result of such access.

- d) The University is free to capture and inspect any data on any networking infrastructure owned by the University.

The University has the right to give to any appropriate member of the

- e) University community, or law enforcement bodies, any information it possesses regarding the use of the University's resources.

These conditions apply to:

- data that is limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets.
- Financial data relating to the operation of the University that, if subject to manipulation or errors, may adversely affect the University.
- Personal data - both staff and student - which is held by the University.

4. Security Management

4.1 Account Management

Information Security Administration

The responsibility for the administration of information security procedures must be assigned to specific personnel in such a way that the procedures can be implemented and monitored while still guaranteeing that the overall security of the University's computing facilities is not compromised.

Responsibilities

The overall responsibility for the management of the security of data rests with the Pro Vice Chancellor - Information Services (PVC-IS).

As part of the security procedures, access to all systems must be monitored on a continuing basis and audit trails or access logs maintained.

Detection and Prevention of Account Misuse

It is in the interests of all account holders that the University negates or minimises any potential or actual security breach. The University may disable an account without notice, regardless of whether the account itself is suspected of misuse.

All other accounts owned by the account holder may also be disabled without notice. The University decides the nature and period of account suspension.

All unsuccessful attempts to logon to University computer systems must be logged and the connection disabled after three unsuccessful attempts.

Terminals which are logged in and inactive for an extended period of time, and which are not being used to process or monitor foreground or background tasks, must be automatically logged off and the details logged for later review.

4.2 Password management

Passwords are a primary defence mechanism on many computer systems. Careful selection of passwords improves security. Individual users are responsible for the robustness and maintenance of their own passwords. Individual users are responsible for the defence of any accounts held by them. The following rules for use of passwords shall apply:

- Passwords must be used where possible
- Passwords must be at least six characters in length.
- A newly-issued password must be changed as soon as possible after issue
- Passwords must be changed regularly, within a period determined by the University
- Passwords must not be displayed next to the terminal.
- Users when logging on must not permit anyone to see their password being entered.
- Passwords must not be disclosed to others
- Passwords should not be easily associated with a particular user.
- Users will not save passwords electronically within applications as far as practically possible.
- A user who realises that a password has been compromised shall change the password, if possible.
The user is required to report all details of the breach to the responsible IT support staff.

Passwords shall be checked by the user to ensure that they comply with guidelines and are non-trivial.

Information on correct selection of passwords shall be readily available and widely distributed.

The use of automatic logons is discouraged.

4.3 Security Breaches

The University will refer any incident involving a possible breach of State, Federal or International law to the appropriate authority for investigation. The University will give that authority all reasonable assistance requested.

If a security breach occurs in which a person or organisation external to the University is involved as a potential victim of the breach, the University will refer to the external party the details specific to that party.

If a security breach involves facilities strictly internal to the University, the University may follow the appropriate University disciplinary procedures.

Security Incident Reviews

The person who carries out the technical investigation of a security breach shall submit a report to the relevant head of section outlining the following details where possible:

- 1 the general nature of the security breach
- 2 the general classification of people involved in the security breach, (such as external client, privileged staff member)
- 3 the computer systems involved in the security breach
- 4 the details of the security breach
- 5 the impact of the security breach
- 6 unrealised, potential consequences of the security breach
- 7 possible courses of action to prevent a repetition of the security breach
- 8 side-effects of those courses of action.

Where appropriate, remedial action should be taken on the basis of this report.

The following steps are listed in the order that they should be taken. Once a breach is confirmed, these steps should be taken as urgently as possible. If a particular step is not appropriate to the breach, then the reader should simply ignore it and move to the next step.

a) The CITO, ITS, should be notified immediately.

If the security breach involves a possible breach of State, Federal or International law, the appropriate authorities should be notified as soon as possible.

If another academic or administrative unit is involved, that unit should be notified as soon as possible, preferably via the Head or an approved representative.

If an organisation or person external to the University is involved in any capacity, then the Australian Computer Emergency Response Team (AUSCERT) should be contacted, where it is deemed necessary by the the CITO, ITD or nominee.

If an organisation or person external to the University is involved as a potential victim, then that organisation or person should be advised as soon as possible.

4.4 Security Audits

Regular auditing procedures shall be carried out on all computer systems to check for conformance to policy, and to satisfy the

a) requirements of the University's internal and external auditors. The depth and regularity of each level of audit should be outlined in the local procedures manual.

- b) Audit procedures, of any level, may be carried out on any computer system at the discretion of the University.

- In the course of the auditing procedure, the University may delete or otherwise modify any data on any computer system that promotes a contravention of this policy or the host configuration guidelines in the local procedures manual, in order to re-establish system security.
- c)

Unauthorised access attempts

All unauthorised access attempts must be noted and logged. The Audit Trail/System Access Log should be reviewed daily, exception reports generated and inspected by the Information Security Officer and appropriate action taken. A copy of the report of unauthorised access attempts must be produced and kept for future reference.

4.5 Disaster Recovery

A disaster recovery plan shall be implemented which takes into account the risk assessment, the University's needs and vulnerabilities. The disaster recovery plan shall be documented and tested periodically.

4.6 Distribution, Review and Amendment of Security Policy

This policy shall be :

- Distributed to designated officers, who shall receive registered copies.
- Reviewed at least annually.
- May be amended as required.
- When amended, each registered copy of the former policy shall be replaced by a copy of the new policy.
- Available on the UNE World Wide Web pages.

4.7 Training

The level of security that can be implemented within the University depends to a large extent on the understanding and co-operation of all staff. The key to good security is based on staff awareness and training.

Personnel who have been granted access to computer systems have a responsibility for the safe keeping of data within their own area of work. Users must be aware of the ways in which the security of data can be enhanced.

To assist staff to gain an understanding of how system security can be enhanced it is necessary to:

- define personnel policies and procedures.
- provide education and appropriate supervision.
- ensure an understanding of confidentiality requirements.

It is essential that all aspects of IT security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal staff induction procedures for all new staff and be conveyed to existing staff on a regular basis.

Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to data that is not required as part of their normal duties.

APPENDICES APPENDIX 1

DEFINITIONS

Account - the login identifier and associated resources for a computer system or application system. Note that in some implementations, an account may be used by a person for a particular purpose even if the person has not actually gone through the login process. Non-multiple-user computer systems are considered to consist of a single account.

Computer System - any device that utilises a central processing unit and the operating system associated with that device. This includes computer networking and remote management equipment as well as traditional computer systems.

PVC - Pro Vice Chancellor or an agent of the Pro Vice Chancellor

CITO, ITD - the Chief Information Technology Officer or an agent of the CITO

Element - a faculty, college, office or other distinct organisation within the University.

External User - a user who is not a University staff member, Postgraduate student or Undergraduate Student of the University.

Faculty - an academic or administrative faculty of the University other than INS.

Filter - a logical or physical device used to selectively permit or deny communications between particular computer systems.

Firewall - a device interconnecting computer systems or networks with the purpose of providing the capability to filter network traffic between those computer systems or networks.

General Access - the availability of a resource to any user.

General Access Laboratory - a laboratory of computer systems that are available for use by any member of the University community.

General Purpose Computer System - any computer system made available for the use of the general University community for approved activity.

ITD - Information Technology Division

Login - the act of accessing a computer system or its associated application systems.

Login Directory - the directory owned by an account on a computer system for the purposes of initial access immediately following the login procedure to access that computer system.

Privileged Account - an account which is capable of carrying out operations that affect the working environment of other accounts. It is normally authorised for use by a restricted group of people who are responsible for computer system administration.

Resource - any computer system, associated networking infrastructure, or service offered by these.

University - the University or appointed officer delegated by the University the responsibility of managing a particular resource on behalf of the University.

Restricted Access Laboratory - a laboratory of computer systems that are available for use by only a restricted, authorised group of people.

Security Breach - a contravention of the IT Security Policy.

System Administrator - any person who is authorised as being responsible for the configuration, maintenance, and operation of a computer system.

Terminal - a physical or virtual device used to access a computer system.

Threat - an event or outcome that may potentially or actually occur as a result of the exploitation of a vulnerability.

University - the University of New England

User - a person using a computer system. A user is normally the account holder of the account being used, but not necessarily so. A person using an account that they are not the holder of and without authority is still classed as a user of the computer system.

User Account - an unprivileged account provided for the use of one authorised person for the purposes of accessing a computer system.

VC - the Vice-Chancellor or an agent of the Vice-Chancellor.

APPENDIX 2

LAW

This section outlines laws and policies that directly shape the IT Security Policy.

The business of the University is constrained and shaped by many laws and policies, some of which indirectly affect the use of computers in the life of the University. It is not the scope of this section to consider laws and policies which fall under this category. For instance, fraud is still fraud whether a computer is involved in the crime or not. In simple terms, this section outlines laws and policies regarding situations in which the computer is the target of the offence, rather than those in which the computer was the tool used to commit the offence.

In all cases, the IT Security Policy is subject to the laws and policies set out in this section.

This section quotes several Acts of Parliament, and refers the reader to corresponding appendices containing the text of these documents. It also offers brief discussions of the implications of these Acts and policies. In all cases, these quotes and discussions have been included in good faith for the convenience of the reader. No responsibility will be accepted by the University for the content of these documents, the accuracy of the quotations from them, or the correctness of the discussions. The reader is directed to refer to the original documents if any guarantee of accuracy is required.

A2.2 Federal Law

Section 76 (in Part VIA - Offences Relating to Computers) of the Crimes Act 1914 details offences regarding Commonwealth computers and facilities. This document is included as Appendix C, Crimes Act 1914, Part VIA - Offences Relating to Computers.

The Act refers to the following offences:

- (a) unlawful access to data in Commonwealth and other computers,
- (b) damaging data in Commonwealth and other computers,
- (c) unlawful access to data in Commonwealth and other computers by means of a Commonwealth facility, and,
- (d) damaging data in Commonwealth and other computers by means of a Commonwealth facility.

The Act implies that the Commonwealth does not need to be the owner of the computer system on which the offence occurred. If data is being held

on the computer system on behalf of the Commonwealth (for instance, to fulfil a lawful requirement), then the offence has still occurred in the context of that section.

The Act also includes offences regarding the use of a Commonwealth facility (such as a Commonwealth supplied communications carrier), regardless of whether the computer is a Commonwealth computer or not. The implications of this may be important when one considers the networking mechanism used to access the computer.

In all cases mentioned above, the Act requires that the person who carried out the activity did so intentionally and without authority.

CRIMES ACT 1914, PART VIA - OFFENCES RELATING TO COMPUTERS

The following material constitutes Part VIA, Offences Relating to Computers (Section 76) of the Commonwealth Crimes Act 1914.

Crimes Act 1914

PART VIA OFFENCES RELATING TO COMPUTERS

Interpretation

SECTION 76A

- 1 In this Part, unless the contrary intention appears:
 - "**Commonwealth**" includes a public authority under the Commonwealth;
 - "**Commonwealth computer**" means a computer, a computer system or a part of a computer system, owned, leased or operated by the Commonwealth;
 - "**data**" includes information, a computer program or part of a computer program.

- 2 In this Part:
 - (a) a reference to data stored in a computer includes a reference to data entered or copied into the computer; and
 - (b) a reference to data stored on behalf of the Commonwealth in a computer includes a reference to:
 - (i) data stored in the computer at the direction or request of the Commonwealth; and
 - (ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.

Unlawful access to data in Commonwealth and other computers

SECTION 76B

(1) A person who intentionally and without authority obtains access to:

- (a) data stored in a Commonwealth computer; or
- (b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer

is guilty of an offence. Penalty: Imprisonment for 6 months.

(2) A person who;

- (a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

- (b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

- (i) the security, defence or international relations of Australia;
- (ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
- (iii) the enforcement of a law of the Commonwealth or of a State or Territory;
- (iv) the protection of public safety;
- (v) the personal affairs of any person;
- (vi) trade secrets;
- (vii) records of a financial institution; or
- (viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence. Penalty: Imprisonment for 2 years

(3) A person who:

- has intentionally and without authority obtained access to data stored in a Commonwealth computer or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;
- (a)

- after examining part of that data knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2) (b); and
- (b)

- (c) continues to examine that data;

is guilty of an offence. Penalty for a contravention of this subsection: Imprisonment for 2 years.

Damaging data in Commonwealth and other computers

SECTION 76C

A person who intentionally and without authority or lawful excuse:

- (a) destroys, erases or alters data stored in, or inserts data into, a Commonwealth computer;
- (b) interferes with, or interrupts or obstructs the lawful use of, a Commonwealth computer;
- (c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or
- (d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

is guilty of an offence. Penalty: Imprisonment for 10 years.

Unlawful access to data in Commonwealth and other computers by means of Commonwealth facility

SECTION 76D

- (1) A person who, by means of a facility operated or provided by the Commonwealth, intentionally and without authority obtains access to data stored in a computer, is guilty of an offence.

Penalty: Imprisonment for 6 months.

(2) A person who:

- by means of a facility operated or provided by the
- (a) Commonwealth, with intent to defraud any person and without authority obtains access to data stored in a computer; or

- by means of such a facility, intentionally and without authority
- (b) obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:
 - (i) the security, defence or international relations of Australia;
 - the existence or identity of a confidential source of information
 - (ii) relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
 - (iii) the enforcement of a law of the Commonwealth or of a State or Territory;
 - (iv) the protection of public safety;
 - (v) the personal affairs of any person;
 - (vi) trade secrets;
 - (vii) records of a financial institution; or
 - (viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

is guilty of an offence. Penalty: Imprisonment for 2 years

(3) A person who:

- by means of a facility operated or provided by the
- (a) Commonwealth, has intentionally and without authority obtained access to data stored in a computer;

- after examining part of that data knows or ought reasonably to know that the part of the data which the person examined relates
- (b) wholly or partly to any of the matters referred to in paragraph (2) (b); and

- (c) continues to examine that data;

is guilty of an offence.

Penalty for a contravention of this subsection: Imprisonment for 2 years.

Damaging data in Commonwealth and other computers by means of Commonwealth facility

SECTION 76E

A person who, by means of a facility operated or provided by the Commonwealth, intentionally and without authority or lawful excuse:

- (a) destroys, erases or alters data stored in, or inserts data into, a computer;
- (b) interferes with, or interrupts or obstructs the lawful use of, a computer; or
- (c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;

is guilty of an offence. Penalty: Imprisonment for 10 years.

Saving of State and Territory laws

SECTION 76F

Sections 76D and 76E are not intended to exclude or limit the concurrent operation of any law of a State or Territory.

A2.3 State Law

A2.3.1 Queensland

"The Department of Justice published a Green Paper on Computer Crime in 1987. Particular attention was given to the offence of 'misappropriation of property' under the Criminal Code sub-s. 408C(1):

'Any person who dishonestly applies to his own use or to the use of any person -

- (a) property belonging to another; or

property belonging to him, which is in his possession or control (either

- (b) solely or jointly with any other person) subject to a trust, direction or condition on account of any other person,

is guilty of the crime of misappropriation of property.'

The Green Paper expressed the view that this provision was sufficiently broad to embrace the use of computers for unauthorised purposes and the use of a terminal and modem to gain remote access to data banks." [2]

The green paper also discusses damage to property and the value associated with such damage (dealt with by s. 469 of the Code). It continues on to a discussion of the taking of information with the physical removal of the information, including the act of breaking into a computer system. Again, heavy use is made of s. 408C of the Code. [3]

Extracts of these sections of the Code are shown below.

EXTRACTS FROM THE QUEENSLAND CRIMINAL CODE

The following passages are extracts from the Queensland Criminal Code.

Section 408C of the Queensland Criminal Code states,

"[s 408C]

408C. Misappropriation of property.

- 1 Any person who dishonestly applies to his own use or to the use of any person
 - (a) property belonging to another; or
 - property belonging to him, which is in his possession or control
 - (b) (either solely or conjointly with any other person) subject to a trust, direction or condition or on account of any other person,is guilty of the crime of misappropriation of property.
- 2 An offender guilty of the crime of misappropriation of property is liable to imprisonment for five years save in any of the following cases when he is liable to imprisonment for ten years, that is to say :-
 - (a) if the offender is a director or member of the governing body of any corporation or company, and the property dishonestly applied belongs to that corporation or company or came into the possession or control of the offender on account of that corporation or company;
 - (b) if the offender is an employee of any other person, and the property dishonestly applied belongs to that other person or came into the possession or control of the offender on account of that other person;
 - (c) if the property dishonestly applied came into the possession or control of the offender subject to a trust, direction or condition

that it should be applied to any purpose or be paid to any person specified in the terms of trust, direction or condition or came into his possession on account of any other person;

- (d) if the property dishonestly applied or the yield to the offender from the dishonest application of the property dishonestly applied is of a value of \$5000 or upwards.

3 For the purposes of this section -

- (a) the term "property" includes money and all other property real or personal, legal or equitable, including things in action and other intangible property;

- (b) a person's application of property may be dishonest notwithstanding that he is willing to pay for the property or that he intends to afterwards restore the property or to make restitution in respect thereof to the person to whom it belongs or to afterwards fulfil his obligations in relation to the property;

- (c) a person's application of property shall be taken not to be dishonest, save where the property came into his possession or control as trustee or personal representative, if when he applies the property he does not know to whom the property belongs and believes on reasonable grounds that such person cannot be discovered by taking reasonable steps;

- (d) persons to whom property belongs include the owner, any part owner, any person having a legal or equitable interest in or claim to the property and any person who, immediately before the offender's application of the property, had control of it."

Section 469 of the Queensland Criminal Code states,

"[s 469]

469. Malicious injuries in general. Any person who wilfully and unlawfully destroys or damages any property is guilty of an offence which, unless otherwise stated, is a misdemeanour, and he is liable, if no other punishment is provided, to imprisonment for two years, or, if the offence is committed by night, to imprisonment for three years."

A2.3.2 NEW SOUTH WALES

CRIMES ACT 1900 - SECT 309

Unlawful access to data in computer

1. A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer is liable,

on conviction before two justices, to imprisonment for 6 months, or to a fine of 50 penalty units, or both.

2. A person who, with intent:
 - (a) to defraud any person; or
 - (b) to dishonestly obtain for himself or herself or another person any financial advantage of any kind; or
 - (c) to dishonestly cause loss or injury to any person, obtains access to a program or data stored in a computer is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

3. A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer, being a program or data that the person knows or ought reasonably to know relates to:
 - (a) confidential government information in relation to security, defence or inter-governmental relations; or
 - (b) the existence or identity of any confidential source of information in relation to the enforcement or administration of the law; or
 - (c) the enforcement or administration of the criminal law; or
 - (d) the maintenance or enforcement of any lawful method or procedure for protecting public safety; or
 - (e) the personal affairs of any person (whether living or deceased); or
 - (f) trade secrets; or
 - (g) records of a financial institution; or
 - (h) information (other than trade secrets) that has a commercial value to any person that could be destroyed or diminished if disclosed, is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

4. A person who
 - (a) without authority or lawful excuse, has intentionally obtained access to a program or data stored in a computer; and
 - (b) after examining part of that program or data, knows or ought reasonably to know that the part of the program or data examined relates wholly or partly to any of the matters referred to in subsection (3); and
 - (c) continues to examine that program or data, is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

CRIMES ACT 1900 - SECT 310

Damaging data in computer

1. A person who intentionally and without authority or lawful excuse:
 - (a) destroys, erases or alters data stored in or inserts data into a computer; or

(b) interferes with, or interrupts or obstructs the lawful use of a computer, is liable to penal servitude for 10 years, or to a fine of 1,000 penalty units, or both.

APPENDIX 3

UNIVERSITY RULES AND DISCIPLINARY PROCEDURES

A3.1 Staff and Students

University rules and disciplinary procedures which apply to staff and students are published in the University handbook and on the Internet World Wide Web pages.

A3.2 Other People

Any person not covered in the above categories will be bound by a verbal or written agreement between that person and the CITO. Any violation of that agreement (or unacceptable behaviour in the absence of an agreement) shall result in appropriate action determined at the discretion of the CITO.

APPENDIX 4

Location of Policy

- Copies of this policy, registered as official and up to date copies, will be held by the Internal Auditor & Cost Center Heads
- An up to date electronic copy will be available on The UNE World Wide Web Pages.
- Copies will be made available to any other UNE staff member or student on request.
- The version current at the time of printing will be included in the UNE Handbook, with the qualifier, "for a current version please consult the UNE World Wide Web Pages".

APPENDIX 5

Acknowledgments

I wish to thank all who took part in the survey of IT security policy last October, particularly Edith Cowan University and Griffith University whose policies have been extensively used and adapted in compiling this draft policy.

I also wish to thank the following for assistance, cooperation and advice:

Professor Joan Cooper, University of Wollongong
Ian Hunter, Executive Officer, CAUDIT
Greg Porter, ITS Director, University of Technology, Sydney

APPENDIX 6

References

Ahuja, V. , ***Network and Internet Security***, Academic Press, Chestnut Hill, USA, 1996

Cheswick, W. and Bellovin, S. , ***Firewalls and Internet Security: Repelling the Wily Hacker***, Addison-Wesley, Reading, USA, 1994

Caelli, W., Longley, D., and Shain, M. , ***Information Security for Managers***, Macmillan, 1989

Edith Cowan University , ***Information Security Policy*** 1996

Griffith University , ***Computer Access Policy*** 1996

Jackson, K.M. and Hruska, J. (eds) , ***Computer Security Reference Book***, Butterworth-Heinemann, Oxford, 1992

National Institute of Standards and Technology (USA) , ***Firewalls FAQ*** (Frequently Asked Questions) 1997

Northern Illinois University, ***Electronic Mail Policy 1996***

Purdue University, ***Electronic Mail Policy 1996***