



Air Niugini Manual Amendment Advice

PART A	
Document Title:	Information Technology Policy and Procedures Manual
Issued To:	Local Area Network (LAN)
Position Title	N/A
Manual Copy No	N/A
Version No	2.1
Revision Date	26/10/22
Distribution Date	27/10/22
Effective Date	10/11/22

INSTRUCTION:

As DOCUMENT HOLDER of this MANUAL –
your responsibility is -

1. to AMEND (Update) this Manual to accurately reflect
The LIST of EFFECTIVE PAGES (LEP) found in the Document Control Section
on Page 5 of this Manual.
2. SIGN and DATE the AMENDMENT RECORD on Page 6.
3. Remove corresponding old pages and replace or add new pages in this version 2.1.
Corresponding old pages are now **OBSOLETE** and **MUST** immediately be removed
4. Do NOT keep previous copies for “reference” or other purposes.
5. BE Prepared for an AUDIT of your Manual at any point in time.

REASON for Changes made to this MANUAL: Refer to Amendment and Review History, page 8.



Air Niugini

Information Technology Policy and Procedures Manual

Information Technology

Document Control No: _____

Confidentiality

This document contains information that is valuable and confidential to Air Niugini and is intended for disclosure to and use by authorised persons only.

If you are not an authorised person, you are notified that any use or dissemination of this information in any manner is strictly prohibited and are requested to either:

Arrange for collection of this document by advising:

Manager Document Production
Air Niugini
Phone: (675) 327 3323

Mail this document to Air Niugini, using the tear-off label shown below.



Postage will be paid
by Air Niugini

Manager Document Production
Air Niugini
PO Box 7186
Boroko NCD
Papua New Guinea



Air Niugini

Document Control

Introduction

Air Niugini based in Port Moresby is the national airline of the Independent State of Papua New Guinea providing air services within Papua New Guinea and throughout Australasia.

This Manual is the controlling document in the Air Niugini **Part 119, 141 and 145 Expositions** under the Papua New Guinea Civil Aviation Rules. It sets out the Air Niugini organisational structure and contains management philosophies, policies and responsibilities that are applicable to all levels of the organisation and to all operations carried out under the Part 119, 141 and 145 Expositions. It also documents specific procedures, such as Internal Audit Procedures and Risk Management, that are applicable across the organisation.

Procedures for the operation of the individual areas of the organisation are documented in subsidiary manuals, such as the Corporate Quality Manual, Flight Administration Manual, Training Policy and Procedures Manual, Engineering Policy and Administration Manual and Design Services Manual that are authorised by this Corporate Policy and Procedures Manual.

Copyright

This publication is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act 2000, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in any retrieval system or transmitted without prior permission of Air Niugini.

All trademarks remain the property of the respective trademark owner.

Authorisation

In accordance with **CAR 119.111(b)**, changes to the items listed below require prior application for and acceptance by the Director. Once the proposal(s) is/are accepted, it/they then can be incorporated into the appropriate parts of the relevant manuals. The Director may amend the conditions on the Air Operator Certificate during or following the changes and Air Niugini is required to comply with all of the conditions prescribed. Where any of the changes requires an amendment to the certificate, the certificate must be surrendered to the Civil Aviation Safety Authority of Papua New Guinea (CASA PNG) as soon as possible.

1. The Chief Executive Officer
2. The listed Senior Persons in the Organisation Structure and
3. The Locations nominated in 119.75(a)(7) from which Air Niugini operates
4. The Scope of the Air Operators Certificate
5. The Maintenance Program
6. Any contractor carrying out the maintenance, training or competency assessment for and on behalf of Air Niugini
7. The Flight and Duty Scheme
8. The Security Program
9. The Fuel Policy
10. Extended Range Operations
11. Safety Management System and
12. Quality Management System

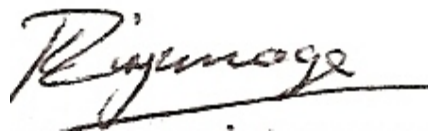
CASA PNG acceptance or approval is indicated by the CASA PNG stamp and the authorised signature. All other pages and changes are approved by the Document Owner in accordance with the Corporate Policy and Procedures Manual.

Release of this document is authorised by the Document Owner:

Title: Executive Manager Information Technology

Name: Kanchana Liyanage

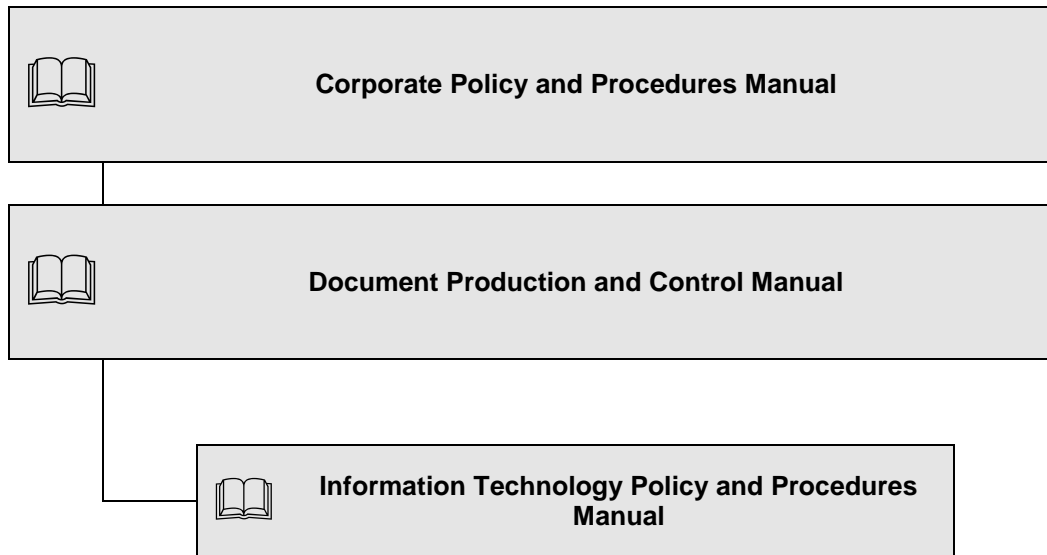
Signature:



Date: 26 October 2022

CASA PNG Acceptance / Approval Not Required

Document Structure

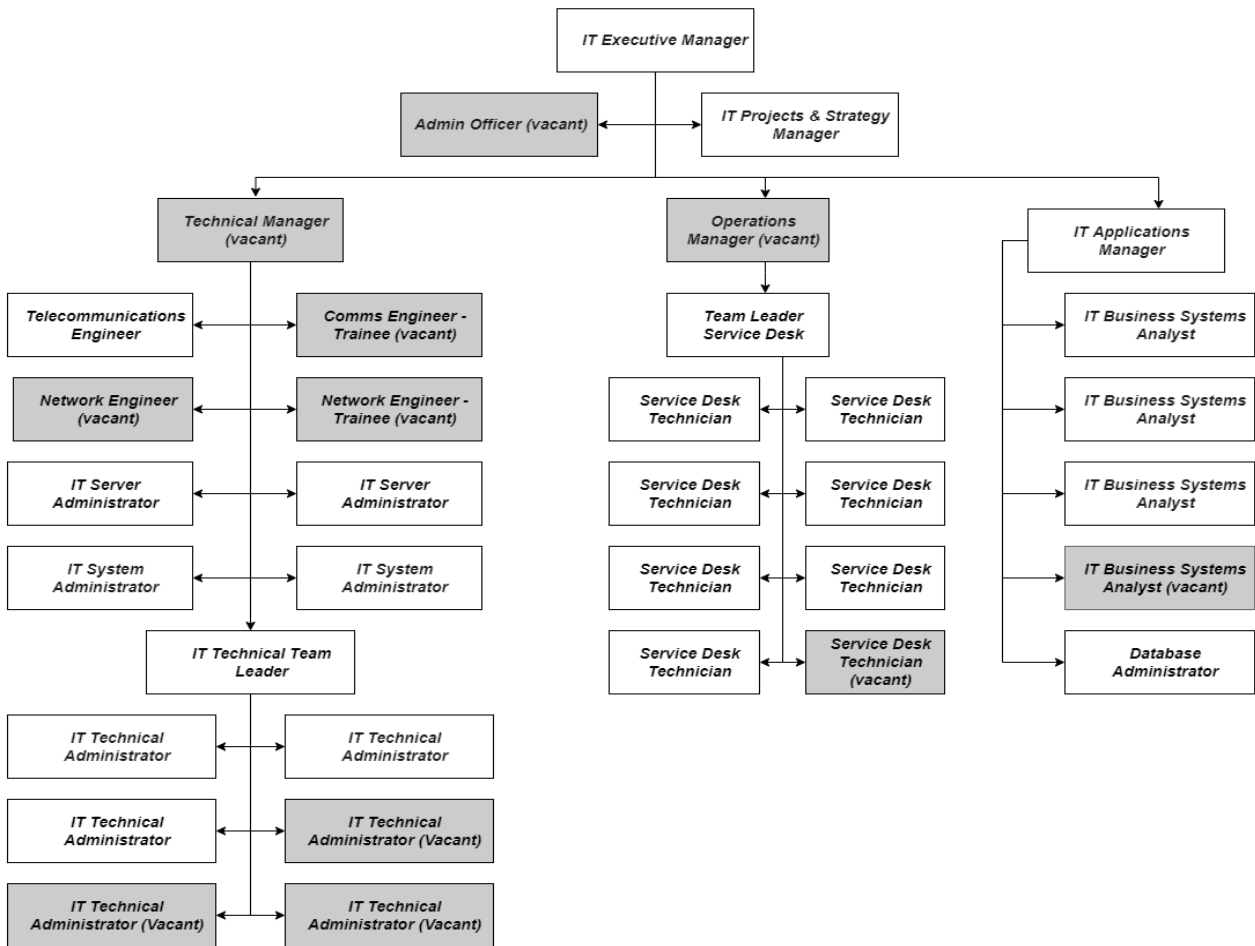


Document Status

Copy status	Controlled
Document owner	Executive Manager Information Technology
Change authority	Executive Manager Information Technology
Change responsibility	Executive Manager Information Technology
Last modified by (optional)	Document Production
Last modified on	26 October 2022

Department Organisation Chart

IT Department Organisation Chart



NOTE: The following documents are saved in the IT Policy folder on the network:

1. ICT-ORG001 IT Department Structure
2. ICT-ORG002 IT Position Descriptions
3. ICT-ORG003 IT Role-Skill Matrix

This part to this folder is \\pomsrvr_itdns01\Information Technology\Administration\IT Policy

List of Effective Pages

Section	Page Numbers	Version Number	Revision Date
Title Page	--	--	--
Confidentiality Notice	--	--	--
Document Control	1 to 16	2.1	26 Oct 2022
1. Code of Ethics	1-1 to 1-8	2.0	1 Jul 2020
2. Information Technology Policy	2-1 to 2-4	2.0	1 Jul 2020
3. Security Policy	3-1 to 3-2	2.0	1 Jul 2020
	3-3 to 3-4	2.1	26 Oct 2022
	3-5 to 3-14	2.0	1 Jul 2020
4. Network Use Procedure	4-1 to 4-4	2.0	1 Jul 2020
5. Email Use Procedure	5-1 to 5-4	2.0	1 Jul 2020
6. Printer and Photocopier Use Procedure	6-1 to 6-2	2.0	1 Jul 2020
7. Administrators' Guidelines	7-1 to 7-2	2.0	1 Jul 2020
8. Data Back-Up Procedure	8-1 to 8-4	2.0	1 Jul 2020
9. Server Room Procedure	9-1 to 9-4	2.1	26 Oct 2022
10. Uninterrupted Power Supply (IT Department) Procedure	10-1 to 10-2	2.0	1 Jul 2020
11. Vendor Management Procedure	11-1 to 11-4	2.0	1 Jul 2020
12. Business Continuity Plan	12-1 to 12-10	2.0	1 Jul 2020
13. Appendix A – Staff Responsibility	13-1 to 13-2	2.1	26 Oct 2022
Document Change Request Instructions	1 to 2	2.0	1 Jul 2020
Document Change Request Form	1 to 2	1.8	30 Jul 2021

Amendment and Review History

Ver No.	Revision Date	Sections changed	Purpose of changes
1.0	1 Aug 12	Original Issue	
1.1	1 May 19	Document Control Pages	Updated Document Control Pages <ul style="list-style-type: none"> • Authorisation Page • Document Structure Page • List of Effective Pages • Amendment Record Page • Amendment and Review History Page
		Page 1	Authorisation Page <ul style="list-style-type: none"> • Position title of Chief Executive Officer has changed to "Managing Director". Per current Org structure <ul style="list-style-type: none"> • Document Owner name has changed to Wendy Henao
		Page 4	Department Org Chart <ul style="list-style-type: none"> • Inserted Department Org Chart. Previously not documented
		4.2.4	Backups <ul style="list-style-type: none"> • Updated of Backups procedure
		4.2.5	Back Up Restoration and Validation <ul style="list-style-type: none"> • Addition of policy Backup Restoration and Validation to validate backed up data.
		8.2.1	Critical Operational Records <ul style="list-style-type: none"> • Deleted SITA in the note section and inserted "Sabre". • Add CHRIS 21 in the examples of electronic system and replaced Mainframe computers with "Virtual Servers". Removed outdated references
			Document Change Request <ul style="list-style-type: none"> • Updated version 1.7 of Document Change Request form is inserted at the back of this manual. Updated form
2.0	1 Jul 20	Document Control Pages	Updated Document Control Pages <ul style="list-style-type: none"> • Inserted updated Dept. Organisation chart. • Added Link to IT Technology\Administration\IT Policy folder. To conform to sect 7 of Corporate Policy & Procedures Manual / Address Internal Audit Finding.
			<ul style="list-style-type: none"> • Entire manual is reissued thus footer of all pages has changed to reflect Executive Manager Information Technology as the Document Owner of this manual.

Ver No.	Revision Date	Sections changed	Purpose of changes
2.1	26 Oct 22	Document Control Pages	<p>Updated Document Control Pages</p> <ul style="list-style-type: none"> Inserted updated. Department Org Chart. <p>Staff move and change over time, thus best to keep positions only in the chart.</p>
		3.2.1.1	<p>Accountability for Information Assets</p> <ul style="list-style-type: none"> Inserted statement after para 2 “All assets will be registered and managed in accordance with the Asset Registry Procedure document. This document is saved in the IT Policy folder on the network”. <p>Per Internal Audit Finding</p>
		9.2.3	<p>Maintenance Register</p> <ul style="list-style-type: none"> Inserted statement after para 1 “Each entry in this register will include an IT Service Desk Incident number. The actions taken and solutions applied will be maintained in the IT Service Desk system, against the referenced incident number.” <p>Per Internal Audit Finding</p>
		13	<p>Appendix A - Staff Responsibility</p> <ul style="list-style-type: none"> Added new heading as Appendix A – Staff Responsibility Subheading to include “Damaged, Lost, or Stolen Assets” and “Employees Leaving or Internal Transfer”. <p>Per Internal Audit Finding</p>
		DCR	<ul style="list-style-type: none"> Inserted updated Document Change Request form version 1.8 dated 30 July 2021. <p>Updated form</p>

Definitions and Abbreviations

Term	Definition
Authorised access	Employees, contractors, consultants and temporary workers who have been granted permission by a manager or supervisor to access computer systems or restricted IT areas, e.g. the Company's server room(s).
Communication	Messages transmitted via technology including personal computers, email, Personal Data Assistants (PDAs), mobile telephones and desktop telephones.
Employees	All Air Niugini staff, contractors, consultants and temporary workers.
Email	Electronic mail, messaging or variants thereof (including email, instant messaging and peer-to-peer file exchange) transmitted or distributed via technology belonging to Air Niugini.
Internet	A global network of computers that are linked together. It allows the exchange of information between business, the Government, education and personal computer users.
Intranet	A network of computers within an organisation that facilitates the exchange of information. Typically, an intranet would allow access to information such as policies, forms, databases and internal news.
IT	Information Technology.
IT Administrator	An employee servicing IT systems who has network or system access over and above normal user access.
Manager	An individual employee's direct supervisor/manager.
Megabyte	A measure of electronic storage capacity/usage. One mega byte approximately equals the 'space' required to store a document containing one million letters or numbers.
Network	Includes all network architecture and infrastructure, personal computers, laptops, servers, printers and any other device attached to the network or a networked device. Networked devices also include any device connected to the network via physical, wireless or other mobile data means, including NextG connections, Blackberry GPRS connections etc.
PC	Personal computer.
Unauthorised access	Employees, contractors, consultants and temporary workers who access computer systems or restricted IT areas, e.g. the Company server room(s), without the appropriate permission of a manager or supervisor.
Vendor	Any person or organisation that maintains, processes or otherwise is permitted access to IT equipment and or information stored on Company network services through its provision of services directly to the Company.



Table of Contents

1.	Code of Ethics	1-1
1.1	Introduction	1-1
1.1.1	General Statement of Policy	1-1
1.1.2	Purpose	1-1
1.1.3	Scope	1-1
1.1.4	Enquiries and Faults	1-1
1.2	Policy	1-2
1.2.1	Company Responsibilities	1-2
1.2.2	Employee Responsibilities	1-2
1.2.3	Authorised Access	1-2
1.3	Responsible Use	1-3
1.3.1	Electronic Mailing Lists	1-3
1.3.2	Network Use	1-4
1.3.3	Representing the Company	1-5
1.3.4	Respect for Other Users of IT Resources	1-6
1.3.5	Privacy	1-7
1.3.6	Copyright Compliance	1-8
1.4	Breach of this Policy	1-8
1.5	Policy Review	1-8
1.6	Authority and Responsibility	1-8
2.	Information Technology Policy	2-1
2.1	Introduction	2-1
2.1.1	General Statement of Policy	2-1
2.1.2	Purpose	2-1
2.1.3	Scope	2-1
2.1.4	Enquiries and Faults	2-1
2.2	Policy	2-2
2.2.1	Company Responsibilities	2-2
2.2.2	Employee Responsibilities	2-2
2.2.2.1	Appropriate Use	2-2
2.2.2.2	Internet Access	2-2
2.2.2.3	Email	2-2
2.2.2.4	Approved Software	2-2
2.2.2.5	Data Storage	2-3
2.2.2.6	Monitoring and Examination	2-3
2.2.2.7	Offensive, Discriminatory and Intimidating Material	2-3
2.2.2.8	Defamation and Harassment	2-3
2.2.2.9	Copyright and Software Licences	2-3
2.2.2.10	Music Downloads	2-4
2.2.2.11	Password Security	2-4
2.2.2.12	Transmission of Sensitive Information	2-4
2.3	Breach of this Policy	2-4
2.4	Policy Review	2-4
2.5	Authority and Responsibility	2-4
3.	Security Policy	3-1
3.1	Introduction	3-1
3.1.1	General Statement of Policy	3-1
3.1.2	Purpose	3-2

3.1.3	Scope.....	3-2
3.1.4	Enquiries and Faults.....	3-2
3.1.5	Roles and Responsibilities.....	3-3
	3.1.5.1 Management Responsibilities.....	3-3
	3.1.5.2 Employee Responsibilities.....	3-3
3.2	Policy.....	3-4
3.2.1	Information Assets Classification and Control.....	3-4
	3.2.1.1 Accountability for Information Assets.....	3-4
	3.2.1.2 Information Asset Classification.....	3-4
	3.2.1.3 Information Owner Responsibilities.....	3-5
3.2.2	Personnel Security.....	3-5
	3.2.2.1 Security in Job Definition and Resourcing.....	3-5
	3.2.2.2 Security Awareness and Training.....	3-5
3.2.3	Physical Security.....	3-6
	3.2.3.1 Secure Areas.....	3-6
	3.2.3.2 Fixed Equipment Security.....	3-6
	3.2.3.3 Portable Equipment Security.....	3-6
3.2.4	Access Controls.....	3-7
	3.2.4.1 Business Requirements for System Access.....	3-7
	3.2.4.2 User Access Management.....	3-7
	3.2.4.3 User Responsibilities.....	3-7
	3.2.4.4 Network Access Control.....	3-8
	3.2.4.5 Application Access Control.....	3-8
	3.2.4.6 Monitoring System Access and Use.....	3-8
3.2.5	Computer and Network Management.....	3-9
	3.2.5.1 Managing the Network.....	3-9
	3.2.5.2 Procedures and Responsibilities.....	3-9
3.2.6	Allocation of Information Security Responsibilities.....	3-9
	3.2.6.1 System Maintenance.....	3-9
3.2.7	Virus Protection.....	3-10
3.2.8	Processing, Transferring and Storing Data.....	3-10
	3.2.8.1 Managing Data Storage.....	3-10
	3.2.8.2 Managing Databases.....	3-10
	3.2.8.3 Managing Confidential Data.....	3-11
	3.2.8.4 Saving Data by Individual Users.....	3-11
	3.2.8.5 Transferring/Exchanging Sensitive or Confidential Data.....	3-11
3.2.9	Systems Development.....	3-12
	3.2.9.1 Security Requirements of Systems.....	3-12
	3.2.9.2 Security in Development and Support Environments.....	3-12
3.2.10	Business Continuity.....	3-12
3.2.11	Security Reviews of IT systems.....	3-13
3.2.12	Security Incident Management.....	3-13
3.2.13	Internal Disciplinary Processes.....	3-14
3.2.14	External Disciplinary Processes.....	3-14
3.3	Breach of this Policy.....	3-14
3.4	Policy Review.....	3-14
3.5	Authority and Responsibility.....	3-14
4.	Network Use Procedure.....	4-1
4.1	Introduction.....	4-1
	4.1.1 Purpose.....	4-1
	4.1.2 Scope.....	4-1
	4.1.3 Enquiries and Faults.....	4-1
	4.1.4 Responsibility.....	4-1

4.2	Procedure	4-2
4.2.1	Instructions for Use.....	4-2
4.2.2	Prohibited Network Use.....	4-2
4.2.3	Network Passwords.....	4-3
4.2.4	Backups.....	4-3
4.2.5	Backup Restoration and Validation	4-3
4.3	Procedure Review	4-3
4.4	Authority and Responsibility	4-3
5.	Email Use Procedure	5-1
5.1	Introduction.....	5-1
5.1.1	Purpose	5-1
5.1.2	Scope	5-1
5.1.3	Enquiries and Faults.....	5-1
5.1.4	Responsibility	5-1
5.2	Procedure.....	5-2
5.2.1	Reasonable Use of the Email System.....	5-2
5.2.2	Prohibited Use of the Email System.....	5-2
5.2.3	Spam	5-2
5.2.4	Bulk Email.....	5-3
5.3	Procedure Review	5-3
5.4	Authority and Responsibility	5-3
6.	Printer and Photocopier Use Procedure	6-1
6.1	Introduction.....	6-1
6.1.1	Purpose	6-1
6.1.2	Scope	6-1
6.1.3	Enquiries and Faults.....	6-1
6.2	Printer Use Procedure	6-1
6.2.1	Reasonable Printer Use	6-1
6.2.2	Prohibited Printer Use	6-1
6.3	Photocopier Use Procedure	6-2
6.3.1	Reasonable Photocopier Use.....	6-2
6.3.2	Prohibited Printer Use	6-2
6.4	Procedure Review	6-2
6.5	Authority and Responsibility	6-2
7.	Administrators' Guidelines.....	7-1
7.1	Introduction.....	7-1
7.1.1	General Statement of Policy.....	7-1
7.1.2	Purpose	7-1
7.1.3	Scope	7-1
7.1.4	Enquiries and Faults.....	7-1
7.2	Policy	7-1
7.2.1	Personal and Professional Conduct.....	7-1
7.2.2	Security of Information	7-2
7.2.3	Personal Information	7-2
7.2.4	Disclosure of Information.....	7-2
7.3	Breach of this Policy.....	7-2
7.4	Policy Review	7-2
7.5	Authority and Responsibility	7-2
8.	Data Back-Up Procedure	8-1

- 8.1 Introduction 8-1
 - 8.1.1 Purpose..... 8-1
 - 8.1.2 Scope..... 8-1
 - 8.1.3 Enquiries and Faults 8-1
 - 8.1.4 Responsibility..... 8-1
- 8.2 Procedure 8-2
 - 8.2.1 Critical Operational Records..... 8-2
 - 8.2.2 Other Operational Records..... 8-2
 - 8.2.3 Departmental Back-Up Procedures..... 8-2
 - 8.2.4 Frequency..... 8-2
 - 8.2.4.1 Critical Operational Records..... 8-2
 - 8.2.4.2 Other Operational Records..... 8-3
 - 8.2.5 Remote Storage..... 8-3
- 8.3 Procedure Review 8-3
- 8.4 Authority and Responsibility 8-3
- 9. Server Room Procedure..... 9-1
 - 9.1 Introduction 9-1
 - 9.1.1 Purpose..... 9-1
 - 9.1.2 Scope..... 9-1
 - 9.1.3 Enquiries and Faults 9-1
 - 9.1.4 Responsibility..... 9-1
 - 9.2 Procedure 9-2
 - 9.2.1 Authorised Access 9-2
 - 9.2.2 Unauthorised Access and Visitors..... 9-2
 - 9.2.3 Maintenance Register..... 9-2
 - 9.2.4 Server Room Housekeeping 9-3
 - 9.3 Procedure Review 9-3
 - 9.4 Authority and Responsibility 9-3
- 10. Uninterrupted Power Supply (IT Department) Procedure 10-1
 - 10.1 Introduction 10-1
 - 10.1.1 General 10-1
 - 10.1.2 Purpose..... 10-1
 - 10.1.3 Scope..... 10-1
 - 10.1.4 Enquiries and Faults 10-1
 - 10.2 Procedure 10-1
 - 10.2.1 UPS Devices..... 10-2
 - 10.3 Procedure Review 10-2
 - 10.4 Authority and Responsibility 10-2
- 11. Vendor Management Procedure 11-1
 - 11.1 Introduction 11-1
 - 11.1.1 Purpose..... 11-1
 - 11.1.2 Scope..... 11-1
 - 11.1.3 Enquiries and Faults 11-1
 - 11.1.4 Responsibility..... 11-1
 - 11.2 Procedure 11-2
 - 11.2.1 Appropriate Vendor Conduct 11-2
 - 11.2.2 Prohibited Vendor Conduct 11-2
 - 11.2.3 Vendor Agreements..... 11-3
 - 11.2.4 Records..... 11-3

11.3	Procedure Review	11-4
11.4	Authority and Responsibility	11-4
12.	Business Continuity Plan	12-1
12.1	Introduction	12-1
12.1.1	Response	12-1
12.1.2	Continuation of Critical Services	12-2
12.1.3	Recovery and Restoration	12-2
12.2	Objectives	12-2
12.3	Process	12-3
12.3.1	BCP Governance	12-3
12.3.2	Business Impact Analysis (BIA)	12-4
12.3.2.1	Identify the Mandate and Critical Aspects of an Organisation	12-4
12.3.2.2	Prioritise Critical Services Or Products	12-4
12.3.2.3	Identify Impacts of Disruptions	12-4
12.3.2.4	Identify Areas of Potential Revenue Loss	12-5
12.3.2.5	Identify Additional Expenses	12-5
12.3.2.6	Identify Intangible Losses	12-5
12.3.2.7	Insurance Requirements	12-5
12.3.2.8	Ranking	12-5
12.3.2.9	Identify Dependencies	12-6
12.3.3	Plans for Business Continuity	12-6
12.3.3.1	Mitigating Threats and Risks	12-6
12.3.3.2	Analyse Current Recovery Capabilities	12-6
12.3.3.3	Create Continuity Plans	12-6
12.3.3.4	Response Preparation	12-7
12.3.3.5	Alternate Facilities	12-7
12.3.4	Readiness Procedures	12-8
12.3.4.1	Training	12-8
12.3.4.2	Exercises	12-8
12.3.5	Quality Assurance Techniques	12-9
12.3.5.1	Internal Review	12-9
12.3.5.2	External Audit	12-9
12.4	Response Management Team (RMT)	12-9
13.	Appendix A – Staff Responsibility	13-1
13.1	Damaged, Lost, or Stolen Assets	13-1
13.2	Employees Leaving or Internal Transfer	13-1





1. Code of Ethics

1.1 Introduction

1.1.1 General Statement of Policy

IT resources are essential for accomplishing Air Niugini's financial and operational objectives. Employees are granted shared access to these resources, which must be used and managed responsibly to ensure their integrity, security and availability for appropriate business activities.

This Code of Ethics provides guidance to authorised users for the appropriate use of Company IT resources.

Within this Code of Ethics, IT resources include all computers, electronic communication devices and software owned or leased by the Company and network facilities that link computers within the Company or which provide external access (e.g. to the Intranet and the Internet).

This Code of Ethics applies irrespective of where Company IT resources are accessed and used, and includes use at employees' homes.

This Code of Ethics is intended to operate within, and be consistent with, existing laws and legislation and the organisation's policies in areas such as sexual harassment, discrimination, equal opportunity, freedom of information, copyright, defamation, discipline and misconduct. It is intended to encourage responsible action and good judgment and to protect privacy.

Sanctions will be enforced if employees act irresponsibly and disregard their obligations to other users, or to the organisation as the provider of information technology resources. Inappropriate use of Company-provided IT resources may also result in suspension, expulsion, termination of employment, legal action or other disciplinary action.

1.1.2 Purpose

All employees are responsible for their own conduct when using Company IT systems. Conduct using these systems must meet the professional standards of behaviour expected of an employee of Company, in line with Air Niugini corporate values.

1.1.3 Scope

This policy applies to all Air Niugini staff, contractors, consultants and temporary workers.

1.1.4 Enquiries and Faults

Adherence to this policy will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this policy, or who wish to report a breach of this policy, should contact the Manager, Information Technology.

1.2 Policy

1.2.1 Company Responsibilities

Reasonable Use Determination

Whether or not use was reasonable in a particular circumstance will be a matter to be determined by the employee's manager.

1.2.2 Employee Responsibilities

Employees must use Company-provided IT resources as the business tools required to perform their work and provide efficient service delivery.

Employees who are authorised to permit other people to use Company IT resources must ensure that those people are made aware of the rules governing use of the organisation's IT resources and have them sign or otherwise acknowledge that they will carry out their responsibilities under these rules.

Employees learning of any violation of this Code of Ethics must bring this matter to the attention of their manager or the Executive Manager Information Technology, without delay.

1.2.3 Authorised Access

Employees may only make use of equipment, networks or information for which proper authorisation has been given. Employees are responsible for ensuring that passwords, accounts, software and data are adequately secured and will be held responsible for all activities that originate from their account.

Employees will select secure passwords to protect their access and must not use any means, electronic or otherwise, to discover others' passwords.

1.3 Responsible Use

Company logos and designs are the property of Air Niugini and may only be used for approved company documents.

Internet, instant messaging and email services can only be used for Company purposes and limited personal use.

"Company purposes" includes any activity that is conducted for the purpose of accomplishing Air Niugini's business.

'Limited personal use' means use that is infrequent and brief. This use should generally occur during personal time and should not include uses:

- That require substantial expenditure of time.
- That are for private business or personal gain or profit.
- That impede the efficiency of intranet, internet or email services.
- That clog mailboxes with large numbers of messages.
- That waste Company resources, such as playing games.
- That would violate or breach the Company Code of Conduct.
- That would violate or breach any Company policies, regulations or harm the Company image or reputation.

As a guide, use that occurs more than a few times per day or for periods longer than a few minutes would not be considered 'limited personal use'.

1.3.1 Electronic Mailing Lists

Employees should use Company electronic mailing lists for Company purposes only. It is inappropriate to:

- Mass email messages of a commercial, political, lobbying or fundraising nature.

NOTE: Sending out a mass email for staff fundraising purposes requires the employee's managers permission.

- Forward chain letters or electronic "petitions", or ask recipients to forward messages.
- Send anonymous messages.
- Solicit support (financial or otherwise) for charity, or special causes not connected with Company.
- Send unverified public service announcements (such as virus alerts, unsafe products, lost and found and health alerts).

Any message sent to a Company electronic mailing list must be relevant to the membership of the list.

1.3.2 Network Use

Employees should not use the Company network to access, or to attempt to access, inappropriate internet sites, regardless of whether such access or such an attempt to access occurs at a Company site or another site (including at home).

Inappropriate internet sites include, but are not limited to:

- Sites that are illegal or hold illegal content.
- Sites that are pornographic or contain inappropriate sexual material .
- Sites that advocate hate or violence.
- Sites that might bring the organisation into disrepute or harm its reputation.
- Sites that offer games or software that are unrelated to Company business.

NOTE: A large number of inappropriate sites are blocked by the Company's Internet filtering software. It is not a defence for an employee who attempts to access a site which is clearly inappropriate for the employee to state they knew the site would be blocked.

Employees must not:

- Attempt to circumvent or subvert system or network security measures.
- Propagate viruses knowingly or maliciously.
- Detrimentally affect the productivity, integrity or security of Government systems.
- Obtain files from unauthorised or questionable non-company sources (e.g. racist material, pornography or file swapping sites).
- Download, distribute, store or display offensive or pornographic images or statements or other material obtained from inappropriate internet sites.
- Download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity and political beliefs.
- Access radio stations or video clips (typically referred to as "streaming" audio or video) over the internet, unless the access is work-related and authorised.
- Download non-work related files, such as freeware, shareware, movie or music files.
- Divulge, share or compromise their own or another's Company authentication credentials.
- Transmit or otherwise expose sensitive or personal information to the internet.
- Use information and technology resources for commercial solicitation or for conducting or pursuing their own business interests or those of another organisation.
- Distribute hoaxes, chain letters or advertisements.
- Send rude, obscene or harassing messages.

- Send, forward and/or reply to large distribution lists concerning non-Company business (in addition, employees must consider the impact on the network when creating and using large work-related distribution lists).
- Attempt to obscure the origin of any message or download material under an assumed internet address.
- Attempt to "spoof" an email (i.e. construct electronic communication so it appears to be from someone else).

Employees must:

- Comply with all applicable legislation, regulations, policies and standards.
- Use all appropriate anti-virus precautions when accessing non-company data and systems from the Company network.
- Adhere to licensing agreements for all software used.
- Respect copyright and other intellectual property rights in relation to both programs and data.
- Only use the email account provided from the Company network when exchanging email with outside systems.
- Use approved security measures when accessing the Company network from home or a non-Company computer.
- Use Company rules for passwords to create passwords.
- Keep personal use of Company IT resources to a minimum.

Any content created or transmitted using Company equipment or retained within the Company network will be managed as a Company record. There is no expectation of personal privacy related to the use of Company IT resources except for specific privileged communications (i.e. solicitor/client and union representative communications).

Inappropriate use of Company IT resources will be investigated on a case-by-case basis. Individuals misusing Company IT resources are subject to disciplinary action, including dismissal, cancellation of contract and/or legal action.

1.3.3 Representing the Company

When employees are representing the views of the Company, the communication must identify their position within Company. Where the view expressed is the official Company view, the authorised source and author of that view should be identified.

Employees must not express views on behalf of Company without official authorisation to do so, or allow another person to reasonably misconstrue that a personal view represents the official position of the Company. In circumstances where readers might reasonably conclude that a personal view is representative of Company, the user must clearly state that the opinion expressed is that of the writer, and not necessarily that of Company, or words to that effect.

1.3.4 Respect for Other Users of IT Resources

Successful use of Company IT resources depends upon a spirit of mutual respect and cooperation to ensure that everyone has equitable privileges, privacy and protection from interference or harassment.

Employees must respect the privacy of other users and not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other users unless specifically authorised to do so.

Employees must not :

- Intentionally disrupt or damage the academic, research, administrative or related pursuits of others.
- Use email or web pages under their control to provide or communicate obscene materials or material that threatens, harasses, intimidates or singles out individuals or groups for degradation or harassment (this material is in violation of PNG law and Company policies and regulations).
- Display on screens images, sounds or messages that could create an atmosphere of discomfort or harassment to others.
- Knowingly create or propagate a virus, worm or any other form of malicious software.
- Tamper with hardware components or hardware configurations without the express permission of the person(s) responsible for that particular item of equipment. This includes:
 - Workstations, monitors, keyboards and mice.
 - Printers and other peripherals.
 - Network outlets, cabling and other components.
 - Phones.

Employees must respect the integrity of the system and not use Company resources to develop or execute programs that could infiltrate the system, tamper with or attempt to subvert security provisions, or damage or alter the software components of the system.

1.3.5 Privacy

The Company's network, systems and facilities are the property of Air Niugini. Anything sent or received using the Company's network, systems and facilities will therefore be transmitted and stored on Company property.

Accordingly, this material is likely to be reviewed by Company. This applies whether you use Company resources at a Company site, at home or any other location.

Air Niugini therefore reserves the right to monitor both usage and content of email messages and visits to internet sites using Company resources to:

- Identify inappropriate use.
- Protect system security.
- Maintain system performance.
- Protect the rights and property of the Company.
- Determine compliance with Company policy and PNG laws.

Air Niugini also reserves the right to monitor and record network traffic, including:

- Email and internet sites accessed.
- Usage data such as account names, source and destination accounts and sites.
- Dates and times of transmission or access.
- Size of transmitted material.
- Other usage-related data.

This information is used for accounting purposes, troubleshooting and systems management.

Air Niugini reserves the right to inspect, copy, store and disclose the contents of the electronic communications of its employees and other authorised users (e.g. contractors or students on work experience) for the purposes of identifying inappropriate use (upon receiving a complaint, investigation request or allegation of misuse). Following authorisation from appropriate Company management, the Police or other law enforcement agencies, the Company will assist in the investigation of any offence.

The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee or authorised user.

Monitoring and inspection can apply to personal and business use of Company-provided intranet or internet services, and personal and business-related email messages.

Employees should always assume that the Company is aware of, or is able to identify at a later date, any website they visit and any email they send.

1.3.6 Copyright Compliance

The Copyright Act sets out the exclusive rights of copyright owners and the rights of users. In addition, certain uses may be covered by licence agreements to which the Company is party.

It is illegal to place on a web page any pictures or video of people without the permission of the people in the picture or video and/or the copyright owner.

Software programs are protected by the Copyright Act. You do not have the right to make and distribute copies of programs without the specific permission of the copyright holder.

1.4 Breach of this Policy

Air Niugini considers any breach of an employee's responsibilities under this Policy to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via Company IT resources. Offenders may also be prosecuted under PNG laws.

The Company may temporarily remove material from websites or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

Failure to comply with the principles of this policy, or with the supporting procedures and forms, could result in appropriate disciplinary actions, suspension, termination of employment (dismissal), or termination of vendor contracts and agreements. Additionally, individuals may be subject to loss of Company access and privileges, and possible civil and/or criminal prosecution.

1.5 Policy Review

This policy will be reviewed annually or as required to reflect changes in business practice or legislation.

1.6 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



2. Information Technology Policy

2.1 Introduction

2.1.1 General Statement of Policy

The Company is committed to providing its staff with effective technology in order to conduct business in the most efficient manner, including PC equipment, network systems, software applications, email and access to the internet. Information Technology (IT) is critical to the business needs of the Company, enabling it to be effective and productive, delivering numerous products and services to both external and internal customers.

Basic computer literacy and a willingness to use other technology and communication methods to maximum advantage are prerequisites for entry to employment in this organisation.

With the use of this technology, there comes a responsibility. Email and the internet are methods of communication, and like all communications made on behalf of the Company, an appropriate standard of behaviour and security must be maintained.

Air Niugini reserves the right to dismiss an employee who does not adhere to the requirements of this policy.

2.1.2 Purpose

The purpose of this policy is to:

- Ensure that all employees are informed of their rights and responsibilities regarding the use of information technology.
- Ensure that these rights and responsibilities are consistently and transparently applied throughout the Company.
- Ensure the confidentiality, integrity and availability of information, while minimising the risk of loss, by implementing the specific procedures and work instructions which support this policy.

2.1.3 Scope

This policy applies to all staff, contractors, consultants and temporary workers.

2.1.4 Enquiries and Faults

Adherence to this policy will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this policy, or who wish to report a breach of this policy, should contact the Manager, Information Technology.

2.2 Policy

2.2.1 Company Responsibilities

Reasonable Use Determination

Whether or not use was reasonable in a particular circumstance will be a matter to be determined by the employee's manager.

2.2.2 Employee Responsibilities

2.2.2.1 Appropriate Use

All employees are responsible for their own conduct when using Company email and IT systems. Conduct using these systems must meet the professional standards of behaviour expected of an employee of the Company in line with Section 1 Code of Ethics.

Company telephones, mobile phones and computers are provided to employees for business use only. Personal usage must be kept to a minimum. Air Niugini reserves the right to charge employees for excessive use of mobile phones. Any damage to Company-owned mobile phones or computers must be reported immediately to the employee's manager.

Computer and internet access is provided to all employees in order to perform work and it is not provided for the personal recreational or personal business use of employees. The computer systems and information contained in those systems belong to Air Niugini. Access to the service will be terminated when the user ceases to be an employee.

2.2.2.2 Internet Access

Access to the internet is primarily intended for business purposes. Access is also permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the Company. Personal use, where necessary, must be kept to a minimum and must not impact an individual's ability to fulfil the requirements of their role. Access to services such as Internet banking and researching formal training courses that are available are examples of acceptable use.

2.2.2.3 Email

Electronic mail is a significant method of communication and, for official purposes, items sent by email will be considered to be equivalent to those sent in writing. All employees are required to read their emails regularly to ensure that important information is received and responded to in a timely manner. Approval from senior management must be gained prior to sending broadcast emails. Senders, recipients and managers of email systems are to exercise due diligence to ensure the protection of confidential communications.

All employees must abide by Section 5 *Email Use Procedure*.

2.2.2.4 Approved Software

The purchase and installation of unapproved software presents risks to the **Company**, such as virus infection, licensing issues or PC problems through incompatibility. Therefore, the purchase and installation of any software requires approval from the Executive Manager Information Technology.

2.2.2.5 Data Storage

Company email and network storage is provided for business use only. Personal material must not be stored on email or network systems. A moderate amount of personal material may be stored on Company PCs. However, the Company does not take responsibility for the safe storage or recovery of any personal data.

2.2.2.6 Monitoring and Examination

The Company reserves the right to examine material stored on Company systems at any time and without prior notice, including but not limited to email messages, personal computer files and other information stored on, or passing through, the Company's computer network.

The Company reserves the right to block or terminate a user's access if there is a practice or information which is not in accordance with organisational policy or where a critical risk has been identified as causing performance or security issues.

2.2.2.7 Offensive, Discriminatory and Intimidating Material

Employees must not access, view, store, transmit, download or create any material that might be deemed:

- **Offensive:** this applies to any material that is violent, sexually explicit, suggestive or racist, and includes swearing and other inappropriate behaviour.
- **Discriminatory:** this includes material that can be deemed discriminatory based on grounds including gender, age, sexuality, race, disability or appearance.
- **Intimidating:** this includes, but is not limited to, personal attacks, threats and messages intended to annoy, harass, intimidate, frighten or alarm people.

2.2.2.8 Defamation and Harassment

To avoid libel, defamation of character and forms of harassment, attacks, threats or messages intended to harass, annoy or alarm another person are strictly prohibited. Items in this category may include, but are not limited to:

- Political statements.
- Religious statements.
- Swearing and other offensive language.
- Statements viewed as harassing to others based on race, religion or beliefs, colour, age, sex, physical disability, politics or sexual orientation.

Management reserves the right to remove any email messages or web pages that have been deemed inconsistent with this policy.

2.2.2.9 Copyright and Software Licences

The Company supports strict adherence to copyrights and software licence agreements. Copying software or copyrighted material in a manner that is not consistent with the vendor's licence or copyright is prohibited.

Copyright infringements are subject to PNG law and have serious legal implications for both the Company and the employee.

2.2.2.10 Music Downloads

The availability of audio-visual material (e.g. music files, films or video) on the internet is not necessarily an indication that the material is copyright free or that it may be downloaded, copied, stored and/or communicated without the specific permission of the copyright owner.

Material that does not support the business purposes of the Company must not be downloaded, copied or communicated using Company equipment or computer networks. This includes music or films that are in digital format and are accessible on internet sites. Posting music or other audio-visual files to the Company website and the transfer of such files to other people within Company, whether by email, memory stick or otherwise, or broadcasting or creating file shares for such material (movies and music) is also unacceptable unless it is for approved Company purposes.

2.2.2.11 Password Security

Employees must keep passwords secure and private. Password should not be easily to guess, and so should not be based on obvious references such as names and birth dates.

If assistance is required, employees should contact the IT Help Desk on ext. 3315 /3583 .

2.2.2.12 Transmission of Sensitive Information

Sensitive information must not be sent over the internet via email unless it has first been encrypted by an approved method to avoid possible interception by third parties.

2.3 Breach of this Policy

Failure to comply with the principles of this policy, or with the supporting procedures and forms, could result in appropriate disciplinary actions, suspension, termination of employment (dismissal), or termination of vendor contracts and agreements. Additionally, individuals may be subject to loss of Company access and privileges, and possible civil and/or criminal prosecution.

2.4 Policy Review

This policy will be reviewed annually or as required to reflect changes in business practice or legislation.

2.5 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



3. Security Policy

3.1 Introduction

3.1.1 General Statement of Policy

The purpose of information security is to ensure the availability of timely and accurate information while preventing and minimising security incidents. To achieve acceptable levels of computer security, Air Niugini has established a systematic approach that considers:

- Confidentiality – protecting sensitive information from unauthorised disclosure.
- Integrity – safeguarding the accuracy and entirety of information and computer software.
- Availability – ensuring that information and vital services are available to users when required.
- Hardware and equipment failure – including a failure of the computer, its storage devices or the network.
- Acts such as fraud, theft, sabotage and misuse of information by employees, suppliers or curious or malicious hackers – to reduce potential losses.

The Company adopts a proactive approach to information security management. Security is a process. It is not possible to buy a single device that will make a network secure, nor a single piece of software that will secure a computer. The process must be applied again and again to a network and the organisation that maintains it.

It is Company policy to ensure that:

- Information is protected and controlled against unauthorised access or misuse.
- The confidentiality of information is assured.
- The integrity of information is maintained.
- Business continuity and planning processes are maintained.
- Statutory, regulatory, legal and contractual requirements are complied with.
- Information security awareness, education and training is provided to all staff.
- Confidentiality statements are issued and signed by all employees.
- All employees and external service providers are held accountable for their actions.
- Information technology assets are classified and protected.
- All information services systems have up-to-date anti-virus software installed.
- Physical, logical and communications security are monitored and maintained.
- Operational policies, procedures and work instructions are maintained.
- All breaches of security are reported to the Executive Manager Information Technology and investigated and handled appropriately.

3.1.2 Purpose

The purpose of this policy is to provide direction and guidance in establishing IT security standards for use within the Company.

3.1.3 Scope

Air Niugini acknowledges an obligation to ensure appropriate security for all IT data, equipment and processes in its domain of ownership and control. This obligation is shared, to varying degrees, by every employee .

The scope of this policy protects (but is not limited to):

- Computer and peripheral equipment.
- Communications equipment.
- Computing and communications premises.
- Communications utilities.
- Supplies and data storage media.
- System computer programs and documentation.
- Application computer programs and documentation.
- Data/Information.

This policy must be broadly communicated to all employees. Awareness is the strongest tool in providing information security. Security is not an end in itself – IT policies and procedures are put in place to protect important assets and thereby support the Company's strategic goals.

3.1.4 Enquiries and Faults

Adherence to this policy will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this policy, or who wish to report a breach of this policy, should contact the Manager, Information Technology.

3.1.5 Roles and Responsibilities

3.1.5.1 Management Responsibilities

Company management shall:

- Ensure that this policy and supporting policies, procedures and work instructions are implemented (as appropriate) at a departmental level, to address all aspects of information security.
- Communicate this policy to all employees and ensure an appropriate level of awareness regarding information security.
- Hold all personnel accountable for their access to and use of information and supporting IT resources.
- Routinely catalogue and value information assets, and assign levels of sensitivity and criticality (information, as an asset, must be uniquely identified and responsibility for it assigned).
- Ensure that information security measures are appropriate to the value of the assets and the threats to which they are exposed.
- Plan for and operate IT in such a way as to preserve the continuity of the Company's operations.
- Take steps to be aware of and address all legal, regulatory and contractual requirements pertaining to information assets.
- Respect the rights and dignity of individuals when setting policies and when selecting, implementing and enforcing security measures.

3.1.5.2 Employee Responsibilities

Technical staff shall:

- Ensure that this policy and supporting best practices and procedures are understood and implemented to address all aspects of information security.
- Respect the rights and dignity of individuals when selecting, implementing and enforcing security measures.

All users shall:

- Be accountable for actions performed on Company systems using their user ID.
- Immediately inform their manager on becoming aware of any loss or any actual or potential compromise of information, or any other incident which has IT security implications.

3.2 Policy

3.2.1 Information Assets Classification and Control

3.2.1.1 Accountability for Information Assets

All major information assets shall be accounted for and have a nominated owner. The nominated owner is authorised to handle that information and is accountable for its safekeeping. In the context of this document, information assets fall into the following categories:

- Data – documented (paper or electronic) information or intellectual assets used to meet the Company's business goals.
- Systems – information technology systems that process and store data. Systems are a combination of information, software, hardware assets and processes. Any host, client, server or network can be considered a system.
- Software – software applications (operating systems, database applications, networking software, office applications, custom applications etc.).
- Hardware – physical devices (workstations, servers etc.).
- Employees – Air Niugini staff and contractors, including their skills, training, knowledge and experience.

Information Technology Department shall maintain and update an asset register of Air Niugini information technology assets. Owners (or custodians) shall be identified for major information assets and assigned responsibility for maintaining appropriate security measures.

All assets will be registered and managed in accordance with the Asset Registry Procedure document. This document is saved in the IT Policy folder on the network.

3.2.1.2 Information Asset Classification

Security classifications shall be used to indicate the need and priorities for security protection. Information assets have varying degrees of sensitivity and criticality, and some items may require an additional level of security protection or special handling.

Confidential or important information assets held by the Company could be lost or destroyed due to inappropriate treatment of information, resulting in the loss of information that is critical to the Company's business activities. If information is not classified to specify its level of sensitivity or confidentiality, then it is very difficult to provide the required level of protection to sensitive information or to meet legal requirements and Company policy in terms of privacy and the treatment of confidential information.

A security classification system shall be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users.

All information, data and documents must be processed and stored in accordance with the classification levels assigned to that information, and must be clearly labelled so that users are aware of the ownership and classification of the information.

3.2.1.3 Information Owner Responsibilities

For security purposes, information shall be assigned an owner. The owner is responsible for:

- Identifying all the information within their area of responsibility.
- Determining the security classification levels of the information.
- Agreeing who can access the information and what type of access each user is allowed.
- Periodically reviewing that classification.
- Ensuring compliance with security controls.
- Ensuring compliance, where necessary, with appropriate legislative and regulatory requirements.

3.2.2 Personnel Security

3.2.2.1 Security in Job Definition and Resourcing

Security shall be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment.

Managers shall ensure that job descriptions address all relevant security responsibilities, and potential candidates shall be adequately screened, especially for sensitive jobs.

All employees and third-party users of Company facilities shall periodically acknowledge (electronically) the IT policies and procedures. This may be accomplished through the user log-in procedure.

Contracts between Air Niugini and third-party vendors shall include the following (refer to Section 11 *Vendor Management Procedure*):

- Confidentiality requirements.
- Adherence to the requirements of Section 3 Security Policy.
- Responsibilities for the management and security of information.
- Ownership of data, software, policies and procedures.
- Clearance of staff where access to classified information is required.

3.2.2.2 Security Awareness and Training

Employees shall be trained in security procedures and the correct use of IT facilities. Air Niugini shall provide induction briefings for all new employees, and new users will receive a copy of all relevant Company policies and procedures upon commencement of work.

All employees will be made aware of the acceptable use procedures for internet, email and other networks. All users must agree and adhere to the IT policies and procedures and the security of Company information.

Network and IT system administrators and technical managers shall receive training on managing network security.

3.2.3 Physical Security

3.2.3.1 Secure Areas

IT facilities supporting critical or sensitive business activities shall be located in secure areas to protect them from theft, fire, flood and other hazards, unauthorised access, damage and interference to IT services.

The unavailability of essential information services will jeopardise normal operations. Accidental damage to premises may also threaten normal business operations. The theft of equipment will not only cause unnecessary expenditure, but may also disrupt the operation of critical systems. Placing equipment in secure areas allows better control of environmental risks.

IT service areas (e.g. programming, system support and security administration) shall be separate from the main computer room.

Server room access is restricted to authorised personnel only, and each person authorised to access the equipment shall be individually identifiable.

Out-of-hours access to the IT environments shall be restricted on an "as-needed" basis.

3.2.3.2 Fixed Equipment Security

Fixed IT equipment shall be protected from security threats and environmental hazards to prevent loss, damage or compromise of assets and interruption to business activities.

Hardware should always be operated under the conditions specified by the manufacturer. Special power supply equipment should be used to ensure that the power supply to sensitive hardware is constant and not subject to surges or drops. Sensitive hardware should not be physically moved unless absolutely necessary, and this should certainly not be on a frequent basis.

Hardware shall not be removed from the premises, unless authorised by the Executive Manager Information Technology.

The serial numbers for all hardware components shall be stored in an asset register, and all hardware failures shall be fully documented and logged. Asset inventory should be conducted on an annual basis to verify that all computer system hardware is accounted for.

Eating and drinking are not permitted in the server room.

3.2.3.3 Portable Equipment Security

Portable IT equipment shall be physically protected from security threats and environmental hazards to prevent loss, damage or compromise and interruption to business activities.

Before portable IT equipment is issued to an employee, the employee must have their manager's approval and be made aware of the security requirements.

Portable IT hardware should always be stored and carried in a purpose-designed carrying case.

Employees shall exercise reasonable caution to ensure the equipment is not left unattended in public places.

Employees shall not store sensitive, confidential or proprietary data on portable IT equipment.

3.2.4 Access Controls

3.2.4.1 Business Requirements for System Access

Access control standards for information systems shall be established by the Company to control access to business information.

Business owners are those most appropriately positioned to understand the nature of information held by a system and who needs to access, enter, update and delete it. Establishing standards and guidelines creates consistency, which makes training more effective and is likely to improve compliance.

Access control standards are rules that are applied to control access to the Company's information assets. Such standards should always be appropriate to the Company's business and security needs.

All information systems shall have a designated owner who is aligned with the business addressed by the system. Information Technology Department shall maintain a register of system owners and oversee the establishment of monitoring and updating standards.

All other access to the Company computer systems shall be granted on a business needs basis. Access to all systems must be authorised by the owner of the system and such access, including the appropriate access rights (or privileges), must be recorded in an Access Control List.

Access Control Lists are to be regarded as highly confidential and safeguarded accordingly.

3.2.4.2 User Access Management

Formal procedures shall be established to control access rights to IT services to prevent unauthorised computer access by assigning a unique user ID to each user of the Company's computer systems.

Access to computer systems shall be via a secure login process designed to minimise the opportunity for unauthorised access.

Requests for granting access rights shall be documented and include authorisation by an appropriate manager. Managers shall also provide timely notification of terminations of contract or temporary staff to the Information Technology Department.

All system access rights must be suspended at the time an employee, contractor or third party leaves the Company. Files and directories created/used by a terminated employee shall either be deleted or reassigned to a replacement user prior to departure.

3.2.4.3 User Responsibilities

All employees have a responsibility to prevent unauthorised user access. Unauthorised access to information systems compromises confidentiality and, potentially, the integrity of the data.

Employees shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

Employees are accountable for the use of **Company** systems performed using their user ID. Employees shall not use another person's user ID and password, and passwords shall be periodically changed as defined in Section 4 *Network Use Procedure*.

3.2.4.4 Network Access Control

Access to the resources on the network must be strictly controlled to prevent unauthorised access and to protect and maintain the integrity of network resources and services. This is necessary in order to ensure that connected users or computer services do not compromise the security of any other networked services.

Controls shall include:

- Appropriate interfaces between networked services.
- Appropriate authentication mechanisms for remote users and equipment.
- Control of user access to IT services.

Any access of internal Company networks shall be regulated by dedicated services enforcing security.

Any user outside the internal Company networks shall not be permitted to connect directly to any resource located on the internal network. Access shall be via a managed firewall or a dedicated service enforcing security.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

3.2.4.5 Application Access Control

Logical access controls shall be used to control and monitor access to application systems and data to prevent unauthorised access to information.

High-risk systems require more stringent access control safeguards due to the confidentiality of the information they process and the purpose of the system. Access controls for highly sensitive information or high-risk systems shall be set in accordance with the value and classification of the information assets being protected.

Logical access to computer software and data shall be restricted to authorised users. Application systems shall:

- Control user access to data and application system functions, in accordance with a defined business access policy.
- Provide protection from unauthorised access for any utility software that is capable of overriding system or application controls.
- Not compromise the security of other systems with which IT resources are shared.
- Review user access rights periodically.

3.2.4.6 Monitoring System Access and Use

System access and use shall be monitored to ensure conformity to policies and standards, and to ensure unauthorised activities are prevented and, if breaches occur, that they are quickly detected.

System access shall be monitored regularly to thwart attempts at unauthorised access and to confirm that access control standards are effective.

For systems where intrusion would have serious consequences, specialist software is to be used.

3.2.5 Computer and Network Management

3.2.5.1 Managing the Network

IT Administrators shall maintain the Company IT network, in order to preserve its integrity and ensure the correct and secure operation of computer and network facilities.

IT Administrators are responsible for overseeing the day-to-day running of the servers and network. This entails ensuring that the computer systems are available and appropriately configured to perform required tasks.

An IT Administrator who lacks the relevant knowledge, experience and training may make errors. The high degree of discretion inherent in the IT or System Administrator's job in itself poses a security threat. Therefore, all IT Administrators shall be properly trained and have adequate experience in the systems and platforms they manage.

In addition, they must be knowledgeable and conversant with the range of information security risks that need to be managed.

IT Administrators shall work in collaboration with system owners.

3.2.5.2 Procedures and Responsibilities

Procedures and responsibilities for managing and operating all computers and networks shall be established and documented to ensure the correct and secure operation of computer and network facilities.

System documentation is a requirement for all information systems, and shall be kept up-to-date and available. Clearly defined procedures and responsibilities ensure that computer systems are available and appropriately configured to perform required tasks.

Responsibilities of IT Administrators shall be clearly documented (refer to Section 7 *Administrators' Guidelines*).

3.2.6 Allocation of Information Security Responsibilities

3.2.6.1 System Maintenance

System maintenance schedules shall be formally planned, authorised and documented to maintain the integrity and availability of information services.

Routine procedures shall be established for:

- Logging events and faults.
- Applying operating system patches.
- Monitoring operational audit logs.
- Monitoring the equipment environment.

System clocks shall be regularly synchronised.

Only qualified and authorised staff or approved third-party technicians may repair information system hardware faults. Modifications to routine systems operations shall be fully tested and approved before being implemented.

3.2.7 Virus Protection

Precautions are required to prevent and detect the introduction and propagation of viruses or malicious software in order to safeguard the availability and integrity of software and data.

A range of techniques has been developed to exploit the vulnerability of computer software to unauthorised or unknown modification, with names such as "computer viruses", "network worms", "Trojan horses" and "logic bombs".

Information Technology Department shall provide anti-virus software for all servers, workstations, notebooks and PDAs.

IT Administrators shall run anti-virus scans on all network file servers, desktops and PCs on a regular basis, and shall be responsible for promptly removing viruses and investigating their origin.

All workstations shall run anti-virus software that is kept up to date, with virus definitions being updated at least weekly.

3.2.8 Processing, Transferring and Storing Data

3.2.8.1 Managing Data Storage

Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need.

Air Niugini's business activities can be severely disrupted if important data becomes unavailable due to deletion. Therefore, all data storage units are backed up on a daily, weekly and monthly basis. Backups shall be to media that can be taken off-site.

When a backup has been taken to removable media, it should be stored in a secure and fireproof location.

Permission to access files shall be granted only by their owner. Read access to files should be restricted to those users who require access to the information for their job function. Update access to files should be restricted to those users who require reading and updating the information for their job function.

3.2.8.2 Managing Databases

The integrity and stability of the Company's databases must be maintained at all times to prevent loss, modification or misuse of data.

Air Niugini depends on data such as personnel records, customer and client records, accounting data, project information and purchases, most of which is held in databases.

Regular processes shall be established to ensure the integrity of data and database indexes. Security measures must not be revoked during the installation or maintenance of databases.

An audit capability should be implemented for all security-related events (e.g. file/folder violations or registry/system reconfigurations). All file/folder access violations should be audited on a regular basis.

3.2.8.3 Managing Confidential Data

Additional measures shall be taken to protect data designated as confidential to prevent loss, modification or misuse.

Confidential information shall only be processed by authorised personnel, and shall be safeguarded using a combination of technical access controls and robust procedures, supported by internal audit controls.

Where databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation.

Permission to access files shall be granted only by their owner. Read access to files should be restricted to those users who require access to the information for their job function. Update access to files should be restricted to those users who require reading and updating the information for their job function.

The authority to create and delete files should only reside with the owner of the data or with those users granted this right as part of their job function.

Testing should not be performed on copies of "live" (production) files that contain sensitive data.

3.2.8.4 Saving Data by Individual Users

Saving data in a structured and timely manner is good practice for all users of computer systems.

All users of information systems must save their work on the network in accordance with best practice. Storing work on the network will prevent loss or corruption of data through system or power malfunction and backup procedures.

Saving data on a local workstation disk (e.g. the C: drive) may appear more convenient but it can frustrate access by other employees who need access to data that is not backed up by a central process. Therefore, data should not be saved to a local hard disk (e.g. C: or D: drive).

Information and data stored on local disks (e.g. notebook computers) must be backed up regularly. It is the responsibility of the employee to ensure that this takes place on a regular basis.

3.2.8.5 Transferring/Exchanging Sensitive or Confidential Data

Sensitive or confidential data and information shall only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be assured.

Where security measures have not been adequately deployed, sensitive information may be accessed by unauthorised persons. The inappropriate and possibly illegal release of information may result in legal action and prosecution.

Data exchanges shall be carried out only after formal approval is given, and procedures and standards to protect media in transit shall be established.

3.2.9 Systems Development

3.2.9.1 Security Requirements of Systems

Security requirements for applications systems shall be identified and agreed prior to developing or enhancing systems to ensure that security is built in. Security requirements shall be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case.

Security considerations will also form part of the technical design for all proposed systems. The design and operation of systems shall conform to commonly accepted industry standards of good security practice.

Security measures shall be determined on the basis of specialist security advice, taking account of identified security threats and their possible business impact.

3.2.9.2 Security in Development and Support Environments

Project and support environments shall be strictly controlled to maintain the security (integrity, confidentiality and availability) of application system software and data.

Managers who are responsible for application systems shall also be responsible for the security of the project or support environment.

Managers shall ensure that all proposed system changes are reviewed and documented to ensure that they do not compromise the security of either the system or the operating environment.

Formal change control procedures shall be utilised for all changes to systems. All changes to programs must be properly authorised and tested before moving to the live environment.

3.2.10 Business Continuity

A Business Continuity Plan shall be available to protect critical business processes from the effects of major failures or disasters (refer to Section 12 *Business Continuity Plan*).

Well-developed and maintained plans for the prompt restoration of critical business processes and services in the event of a business interruption will minimise the impact. Interruptions may be caused by natural disasters, accidents, equipment failures, deliberate action, loss of supplied services or loss of utilities.

Business continuity planning shall include measures to identify and reduce risks, limit the consequences should a threat be realised, and ensure a speedy resumption of essential operations.

Plans shall be reviewed and tested to ensure that the recovery target times for systems remain appropriate to the business tolerance period.

3.2.11 Security Reviews of IT systems

The security of IT systems shall be regularly reviewed to ensure compliance with Company's security policies and standards.

Monitoring is one of the most important aspects of IT security. Implemented safeguards must be used correctly and any security incidents and changes must be recorded, detected and dealt with.

Maintenance activities shall include:

- Allocating resources to maintain safeguards.
- Clearly establishing responsibility for maintaining safeguards.
- Periodically verifying the effectiveness of security safeguards.
- Periodically checking log files.
- Upgrading safeguards when new requirements are discovered.
- External and internal security audits.
- Third-party vendor security audits.
- Modifying parameters and documentation to reflect changes.

Spot checks shall be performed to determine whether support staff and users are conforming to specific safeguards and procedures. Where some safeguards are not effective or complied with, a corrective action plan shall be produced, activated and the results reviewed.

3.2.12 Security Incident Management

When a security breach occurs, the problem needs rapid control and a return to normal operations as soon as possible.

When a security breach occurs, the problem needs rapid control and a return to normal operations as soon as possible.

Any person who becomes aware of any loss, compromise or possible compromise of information, or any other incident which has IT security implications, shall immediately inform their manager, who shall advise the Executive Manager Information Technology. The Executive Manager Information Technology shall initiate immediate action to prevent further compromise or loss, and the manager shall ensure that the violation is investigated.

When the investigation is complete, the Executive Manager Information Technology shall consider the recommended remedial action and take steps to prevent further breaches.

All security incidents shall be recorded to ensure that details of the incident, investigation, resolution and outcome are documented.

3.2.13 Internal Disciplinary Processes

A formal disciplinary process shall be established for dealing with employees who commit a security breach.

The extent of disciplinary action to be taken where a violation has occurred depends on a number of factors. These factors include the severity of the violation, the extent of the supporting evidence, the mechanisms used to achieve the breach, the nature of the data being violated and whether the violation is perceived to have been made by an employee.

Both internal and external disciplinary measures may be available depending on the type of violation that occurred. The course of disciplinary action to be undertaken must be determined by the Executive Manager Information Technology in conjunction with the employee's manager on a case-by-case basis.

Section 1 Code of Ethics defines the behaviour expected of employees when utilising information and actions that may be taken in the event of breaches.

3.2.14 External Disciplinary Processes

Independent of whether the security violation is an internal or external matter, where it is considered a criminal offence, the Police shall be informed.

The decision to involve Police shall be determined by the Chief Executive Office. There shall be adequate evidence to support an action against a person or organisation. Where the action involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard.

3.3 Breach of this Policy

Failure to comply with the principles of this policy, or with the supporting procedures and forms, could result in appropriate disciplinary actions, suspension, termination of employment (dismissal), or termination of vendor contracts and agreements. Additionally, individuals may be subject to the loss of Company access and privileges, and possible civil and/or criminal prosecution.

3.4 Policy Review

This policy will be reviewed annually or as required to reflect changes in business practice or legislation.

3.5 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



4. Network Use Procedure

4.1 Introduction

4.1.1 Purpose

The purpose of this procedure is to define suitable usage and access for the effective and appropriate use of the Company's network services.

4.1.2 Scope

This procedure is relevant to all staff, contractors, consultants and temporary workers, to ensure that network services are used in an appropriate manner.

4.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

4.1.4 Responsibility

Network services are provided for the conduct of the Company's business activities. Air Niugini accepts that limited use of the network system for non-work related purposes may occur. Such purposes should be kept to a minimum and should not interfere with work.

Air Niugini will endeavour to protect the confidentiality of information and material furnished by users and will instruct all computing personnel to protect the confidentiality of such information and material, but the Company shall be under no liability in the event of any improper disclosure.

The use of the computing and networking facilities is permitted by the Company on the condition that it will not involve the infringement of any patent or the breach of any copyright that may be brought or made against the Company or any member of its staff, arising out of or in connection with the use of the computing and networking facilities.

It is the policy of the Company that its computing and associated network facilities are not to be used for commercial purposes or non-Company related activities without written authorisation from the Executive Manager Information Technology.

The Company:

- Provides a safe, secure and backed-up central file storage with individual quotas for staff to store their work data. This file store has no single point of failure and hence is highly available.
- Is responsible for managing network drive space including setting quotas for individuals and departments.
- Reserves the right to permanently limit or restrict any employee's usage of the computing and networking facilities to copy, remove or otherwise alter any information or system that may undermine the authorised use of the computing and networking facilities.
- Through authorised individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them. This authorisation must be granted by the Executive Manager Information Technology or delegate IT Department staff member.

4.2 Procedure

4.2.1 Instructions for Use

The network is to be used only by authorised persons who must have been issued a user name and password. Employees shall not disclose their user names or passwords to others and may not use someone else's user name and password without express authorisation from the Executive Manager Information Technology.

All passwords must adhere to the Company's password policy.

Users must not compromise the privacy of their password by giving it to others, exposing it in public view or being negligent in divulging this information. A user is responsible for all activity on the network performed under their login.

When leaving a PC unattended for any length of time users must lock the computer (if applicable to the Windows operating system running on the PC) or must log off, preventing anyone else from using the computer under their login.

Network access may be suspended or removed from staff who are absent for extended periods, including Long Service Leave, Parental Leave or suspension unless prior approval is granted by Executive Manager Information Technology.

All laptop and desktop computers are to display the Company-approved and issued desktop. Users must not alter, replace or remove this desktop for any purpose not expressly authorised by the Executive Manager Information Technology.

Software, applications, add-ins, automated or manual scripts or any other form of installation must not be installed, activated or stored on any Company PC without the express authorisation of the Executive Manager Information Technology. This includes, but is not limited to, personal software, individually licensed software, freeware, shareware or system scripts.

All desktops, laptops and monitors should be switched off when not in use, for example overnight or off-shift.

4.2.2 Prohibited Network Use

In general, it is inappropriate use to store and/or give access to information on Company computing and networking facilities that could result in legal action against the Company. The issuing of any such information or data that through its release could result in legal action against the Company must be expressly approved by the corporate data owner.

Company computing and network facilities must not be used to transmit, obtain, possess, demonstrate, advertise or request the transmission of objectionable material.

Company computing and network facilities, including memory sticks, must not be used for viewing, disseminating, storing, sharing or creating any material that is pornographic, lewd, obscene, offensive or discriminatory. This includes video files, images, documents, email content, etc.

Users must not store any file on the Company computing network or on any personal computer that is subject to copyright protection without suitable written consent of the licence holder.

Users should not knowingly possess, give to another person, install or run on any of the computing and networking facilities programs or other information that could result in the violation of any Company policy or the violation of any applicable license or contract. This is directed towards, but not limited to, software known as viruses, Trojan horses, worms, password breakers and packet observers.

Users should not intentionally use the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not any actual message is communicated, or where no purpose of legitimate communication exists and where the recipient has expressed a desire for the communication to cease.

4.2.3 Network Passwords

Network passwords are to be a minimum of eight (8) characters in length, and must include:

- At least one lower-case letter (e.g. "m") and one upper-case letter (e.g. "M").
- At least one number (e.g. "1", "9" or "67").
- May contain punctuation characters (e.g. "!" or "=").

Network passwords are to be substantially changed on a regular basis, e.g. monthly.

NOTE: Changing a password from e.g. "Mosbi001" to "Mosbi002" is NOT a significant change and would be a breach of this policy.

It is recommended that passwords not be any word from the dictionary, names, birth dates or words with an incremental number.

The best passwords are ones containing alpha and numeric and punctuation characters. A good example of a password is the first letter of each of the words of a saying that you know, with a punctuation and numeric character included.

4.2.4 Backups

Files stored on the network/shared drive and servers (database and application) are to be backup up daily and weekly.

The full backup made on the first weekend of the month is kept as a monthly backup. Differential backups (i.e. backups of files changed since the last backup) are made daily (overnight).

4.2.5 Backup Restoration and Validation

A random server is selected to be restored, to validate the data on a weekly basis. This server is further authenticated by Business Analyst responsible for the Application and data on the Backup Restoration Log maintained by Systems Administration.

4.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

4.4 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.





5. Email Use Procedure

5.1 Introduction

5.1.1 Purpose

The purpose of this procedure is to define suitable usage and access for the effective and appropriate use of the Company's email system. Email is a tool for business communications, which users have a responsibility to use in an efficient, effective, ethical and lawful manner. Email is inherently not secure, and sensitive or confidential material should not be sent through the electronic mail system unless it is encrypted. The best practices in this procedure have been developed to maintain:

- Professionalism: employees must act as professionals and must use proper language within emails to convey a professional image.
- Efficiency: employees should create emails that are well written, concise and not ambiguous.
- Protection from liability: employees must be aware of email risks that can contribute to the Company's legal liabilities.

5.1.2 Scope

This procedure is relevant to all staff, contractors, consultants and temporary workers.

5.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

5.1.4 Responsibility

The email system is provided for the conduct of the Company's business activities. Air Niugini accepts that limited use of the email system for non-work related purposes may occur. Such purposes should be kept to a minimum and should not interfere with work.

All users granted access to the Company network automatically have access to the email system. Use of the email system must not contravene any legislation, regulation or Company policy or procedure or be used as a method for delivering offensive or objectionable communications. All information and messages that are created, sent, received or stored on the email system are the sole property of the Company.

Users of the email system are allocated a standard amount of storage on the Company's network. This is referred to as the email quota. Users are expected to manage their email within this quota.

Emails sent via the internet are not secure. There is no guarantee of delivery and a third party may tamper with them. The content of a message can be modified or a message forwarded in a manner that gives the impression of it having originated elsewhere. It is therefore important to assess the authenticity of messages prior to making decisions based upon their contents.

Users should also be aware that by sending messages to open groups, their email address will become public.

5.2 Procedure

5.2.1 Reasonable Use of the Email System

Employees must:

- Ensure that messages are addressed to the appropriate recipient.
- Address messages to recipients who 'need to know', rather than to everyone you know (messages sent unnecessarily can lower system and user performance).
- Construct messages professionally (e.g. with correct spelling and grammar) and efficiently (e.g. using the subject field and attachments) and should not use capital letters unnecessarily.
- Cover periods of absence by using email forwarding or out-of-office alerts.
- Ensure that email is checked at least once during each day or shift, as appropriate.

5.2.2 Prohibited Use of the Email System

Emails may not contain statements or content that is libellous, offensive, harassing, illegal, derogatory or discriminatory. Foul, inappropriate or offensive messages such as racial, sexual or religious chain letters and jokes are strictly prohibited.

Chain letters, jokes and other non-Company video files and images received by email must be immediately deleted and the attachments must not be saved to local or network drives.

The exchange of proprietary information, trade secrets or any other privileged, confidential or sensitive information outside the organisation, or outside a defined privileged group, is strictly prohibited.

The creation and exchange of advertisements, solicitations, chain letters, jokes and other unsolicited email is strictly prohibited.

The creation, storage or exchange of information in violation of copyright laws is strictly prohibited.

Reading or sending messages from another user's account, except under proper delegate arrangements, is strictly prohibited.

Altering or copying a message or attachment belonging to another user without the permission of the originator is strictly prohibited. The only exception to this is to the Systems Administration role where this is performed in the normal course of their duties.

Employees are not permitted request, seek access to or use any other means to gain the password (including electronic capture) of another Company user without the express permission of the Executive Manager Information Technology.

5.2.3 Spam

Employees must not generate or forward electronic messages that could be classified as "spam".

5.2.4 Bulk Email

In general, the use of the Company's email system for the bulk distribution of information (also referred to as "broadcast emails") is discouraged (e.g. 20+ recipients). Any such requirements should be met by the employee sending a request to the Webmaster for the relevant email to be forwarded to the relevant users.

In addition, the following guidelines should be adhered to for bulk email:

- Messages should be plain text with no attachments. (If recipients require another kind of material, it can be posted at a website and links can be included in the message.)
- Distribution lists should be kept private. This can be done by listing recipients in Bcc: address fields instead of To: or Cc: address fields.
- Timing and other details of bulk mailings should be coordinated with the Webmaster.

5.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

5.4 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.





6. Printer and Photocopier Use Procedure

6.1 Introduction

6.1.1 Purpose

The purpose of this procedure is to define appropriate use for Company printers and photocopiers.

6.1.2 Scope

This procedure is relevant to all staff, contractors, consultants and temporary workers, to ensure that printers and photocopiers are used in an appropriate manner.

6.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

6.2 Printer Use Procedure

6.2.1 Reasonable Printer Use

Printers are provided for the conduct of the Company's business activities. Air Niugini accepts that limited use of the printers for personal purposes may occur. However, such purposes should be kept to a minimum and should not interfere with work. The following printing rules have been implemented to minimise environmental impact and costs:

- Recycled paper should be used when available.
- Double-sided printing should be used whenever possible to minimise paper usage.
- Colour printing should be kept to a minimum and only used when required.

All materials to be printed are subject to current copyright laws. The copyright law governs making copies or other reproductions of copyright material. The person using the equipment is liable for any infringement.

If an error arises with a printer that an employee is unable to fix, the error should be reported to the IT Equipment Fault Help Desk on extn. 3315 / 3583.

6.2.2 Prohibited Printer Use

Employees must not:

- Use Company printers for personal gain (e.g. for their own business activities or the business activities of a third person such as a relative or friend).
- Bulk print documents not related to company business (i.e. more than three copies of a document).

6.3 Photocopier Use Procedure

6.3.1 Reasonable Photocopier Use

Photocopiers are provided for the conduct of the Company's business activities. Air Niugini accepts that limited use of photocopiers for personal purposes may occur. However, such purposes should be kept to a minimum and should not interfere with the performance of Company related activities.

All materials to be photocopied are subject to current copyright laws. The copyright law governs making copies or other reproductions of copyright material. The person using the equipment is liable for any infringement.

Photocopiers are to be set to use black and white by default. Colour photocopying (where available) should be kept to a minimum and only used if necessary.

If an error arises with a photocopier that an employee is unable to fix, the error should be reported to the IT Equipment Fault Help Desk on extn. 3315 / 3583.

6.3.2 Prohibited Printer Use

Employees must not:

- Use Company photocopiers for personal gain (e.g. for their own business activities or the business activities of a third person such as a relative or friend).
- Bulk photocopy documents not related to company business (i.e. more than three copies of a document).

6.4 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

6.5 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



7. Administrators' Guidelines

7.1 Introduction

7.1.1 General Statement of Policy

This policy aims to foster and maintain confidence in the integrity and professionalism of IT Administrators by ensuring that they:

- Maintain appropriate standards of conduct.
- Develop, as necessary, those skills necessary for the efficient performance of their duties.
- Maintain fairness and equity in decision making.
- Maintain and enhance the reputation of Air Niugini.

7.1.2 Purpose

The purpose of this policy is to outline the standards of conduct that are expected from IT Administrators at Air Niugini.

7.1.3 Scope

This policy applies to all staff, contractors, consultants and temporary workers.

7.1.4 Enquiries and Faults

Adherence to this policy will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this policy, or who wish to report a breach of this policy, should contact the Manager, Information Technology.

7.2 Policy

7.2.1 Personal and Professional Conduct

The personal and professional behaviour of Air Niugini employees should conform to standards that could reasonably be expected of such persons by virtue of their positions. This includes:

- IT Administrators should serve all staff, contractors and temporary staff in a manner that promotes confidence.
- IT Administrators are committed to performing official duties with professionalism, care, skill, fairness and diligence, and exercise their given authority for the purposes for which that authority has been granted.
- IT Administrators shall use facilities and equipment including computers, email, internet access and mobile phones for official purposes only.
- IT Administrators shall ensure that all resources within their area of responsibility are used effectively and economically in the course of their duties.
- IT Administrators shall treat staff, contractors, vendors and members of the public with courtesy, and with respect for their rights, duties and aspirations.

7.2.2 Security of Information

Staff-related information is confidential. Any information regarding employees or a service shall not be conveyed to another person, without authorisation from their manager.

Confidentiality regarding business or finance information and security of systems information shall be adhered to by all staff.

7.2.3 Personal Information

IT Administrators may collect, use and disclose personal information only where is necessary the performance of their work.

IT Administrators shall take reasonable steps to protect personal information from misuse and loss, and from unauthorised access, modification or disclosure.

7.2.4 Disclosure of Information

IT Administrators should only release information they are authorised to release in the normal course of their duties.

IT Administrators should not release information in a manner which is misleading or which is likely to be misused.

7.3 Breach of this Policy

Failure to comply with the principles of this policy, or with supporting procedures and forms, could result in appropriate disciplinary actions, suspension, termination of employment (dismissal), or termination of vendor contracts and agreements. Additionally, individuals may be subject to loss of Air Niugini access and privileges, and possible civil and/or criminal prosecution.

7.4 Policy Review

This policy will be reviewed annually or as required to reflect changes in business practice or legislation.

7.5 Authority and Responsibility

This policy is issued under the authority of the Manager, Information Technology.



8. Data Back-Up Procedure

8.1 Introduction

NOTE: In this procedure:

- "Data" includes documents, financial records, operational and training records, etc.
- "Critical operational records" are those records used directly or in support of operational functions or activities.

8.1.1 Purpose

The purpose of this procedure is to describe the back-up process used by Information Technology Department to ensure the safeguarding of critical operational records and other data.

8.1.2 Scope

This procedure is relevant to critical operational records and other data created and maintained by all staff, contractors, consultants and temporary workers.

8.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

8.1.4 Responsibility

It is the responsibility of the Executive Manager Information Technology to ensure the back-up requirements described in this section are implemented and are being maintained.

All users are responsible for complying with this procedure.

8.2 Procedure

8.2.1 Critical Operational Records

All electronic systems maintaining critical operational records, e.g. Geneva, AQD and Chris21, are run on the Company's virtual servers or file servers under the control of IT Department (or a contracted service provider).

IT Department (or the contracted service provider) is responsible for ensuring that automatic overnight back-ups are made of these records.

NOTE: As an example of a "contracted service provider system", electronic back-ups of the databases in the Sabre Departure Control System are the responsibility of, and are carried out by, Sabre.

8.2.2 Other Operational Records

All operational files on the company's LAN file servers are automatically backed up onto tape, etc. on an overnight basis, under the control of IT Dept., unless the LAN file remains "in use" on a user's PC. For this reason, users shall close any electronic records maintained on the LAN at the end of the day and shall also close the software program used to open them, e.g. Excel.

Operational records maintained on personal computer hard disks shall be manually backed-up by the relevant users to the company's LAN file servers on at least a weekly basis (for low frequency records that can be reconstructed from paper forms, etc.) or on an end-of-day basis (for high frequency records and/or records that cannot be easily reconstructed from paper forms, etc.).

8.2.3 Departmental Back-Up Procedures

Departments may implement back-up procedures that are in addition to the requirements of this Section.

As an example, Document Production maintains an additional back-up copy of Microsoft Word master files (of Company manuals) on the Document Production office computers, i.e. as well as these files being located on, and being automatically backed up overnight from, the LAN.

8.2.4 Frequency

8.2.4.1 Critical Operational Records

Critical operational data/records must be backed up daily and held for 14 days. The backup for each of the thirteen days can then be overwritten in order. The backup for the fourteenth day is to be kept for at least 2 weeks before reuse.

8.2.4.2 Other Operational Records

Non-critical operational data/records should be backed up on a daily basis but, where this is not practicable, must be backed once each week, and the back-up must be on the same day each week.

For records/data backed up on a daily basis:

- Data must be held for 14 days.
- The backup for each of the non-current thirteen days can be overwritten in order.
- The backup for the fourteenth day is to be kept for at least 2 weeks before reuse.

For records/data backed up on a weekly basis:

- Data must be held for 3 months (i.e. 12 tapes).
- The backup for each of the non-current 11 weeks can be overwritten in order.
- The backup for the twelfth week is to be kept for at least 3 months before reuse.

8.2.5 Remote Storage

Backup tapes shall be stored in a remote location, when not being used to create a back-up or to restore lost data.

8.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

8.4 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.





9. Server Room Procedure

9.1 Introduction

9.1.1 Purpose

The purpose of this procedure is to maintain a high level of security and cleanliness in the IT Department server room(s).

9.1.2 Scope

This procedure is relevant to all staff, contractors, consultants and temporary workers who have authorised access to the IT server room(s).

9.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

9.1.4 Responsibility

It is the responsibility of the Executive Manager Information Technology to maintain a Server Room Access Log.

It is the responsibility of all employees to adhere to this procedure and ensure that they carry out their duties in a professional manner while working in the server room(s).

9.2 Procedure

9.2.1 Authorised Access

Access to the IT Department server room(s) is restricted. Only authorised personnel are allowed to gain entry into the area. Authorised personnel are identified as those people needed to operate, supervise or provide maintenance to the area and its equipment.

The server room(s) is to be locked at all times. All authorised staff are required to be signed in and out of the server room(s) using the Server Room Access Log.

Access to the server room(s) is restricted to IT personnel, approved vendor and maintenance personnel and operations management personnel.

A list of personnel authorised to gain entry into the server room(s) will be maintained by the Executive Manager Information Technology and reviewed every six months (at a minimum).

9.2.2 Unauthorised Access and Visitors

Access to the server room(s) for visitors, employees, vendors or customers must be authorised and approved by the Executive Manager Information Technology.

Visitor access can only be granted during business hours. Visitors are permitted access if escorted by appropriate IT Department personnel at all times.

Access will be granted to appropriate service personnel for the completion of work to repair hardware or software. Access to service personnel can be granted out of hours, but these people must be escorted by appropriate IT Department personnel at all times.

9.2.3 Maintenance Register

A Maintenance Register will be established and maintained for all hardware devices and computer systems in the Server Room, providing a list of all problems, subsequent actions and solutions encountered during the life of the hardware devices and computer systems.

Each entry in this register will include an IT Service Desk incident number. The actions taken and solutions applied will be maintained in the IT Service Desk system, against the reference incident number.

During testing periods, the entries in the register should be used to evaluate the validity of the predetermined end of the testing date.

9.2.4 Server Room Housekeeping

Authorised IT Department personnel are responsible for ensuring the safety and cleanliness of the server room(s) at all times.

The following rules have been established to maintain the security and cleanliness of the server room(s):

- No smoking, drinking or eating is permitted in the server room area.
- A clean working area is to be maintained at all times.
- Items removed for use are to be returned to the area where they belong.
- Shoes must be worn at all times.
- Radios and televisions are not permitted in the server room.
- The computer is not to be used for other than assigned operations.
- Temperature and humidity are to be monitored at all times and kept within the recommended ranges for equipment.

9.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

9.4 Authority and Responsibility

This procedure is issued under the authority of the Manager, Information Technology.





10. Uninterrupted Power Supply (IT Department) Procedure

10.1 Introduction

10.1.1 General

Uninterrupted power supply (UPS) devices allows equipment to be switched to "back-up power" in the event of a failure of primary electrical power.

10.1.2 Purpose

The purpose of this procedure is to provide the minimum requirements for UPS devices and describe IT Department personnel responsibilities to ensure critical hardware systems in the IT Department continue running under back-up power in the event of a power failure.

10.1.3 Scope

This policy applies to all staff and contractors in the IT Department who have responsibilities in their job descriptions for critical hardware systems and/or UPS devices.

10.1.4 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

10.2 Procedure

When there is a lose of primary electrical power, IT Department personnel must take appropriate action to ensure critical hardware systems are switched to back-up power until primary power is restored.

UPS devices must be attached to all critical hardware systems within IT Department. A critical hardware system, for the purposes of this UPS procedure:

1. Is any computer or communications device that runs on a mains electrical power supply and which would otherwise stop functioning during a power blackout.
2. Includes all hardware (running off a mains electrical power supply) in the IT Department Computer Room.

UPS devices must be attached to critical hardware systems in tandem to ensure that, in the event of a UPS device failing during a power blackout, at least one UPS device will continue functioning and will continue to provide the requisite power to the hardware system.

Sufficient UPS devices must be under constant charging, for each critical hardware system, to ensure that:

- Two or more UPS devices in tandem will at all times be ready to provide power to a critical hardware system in the event of a power blackout.
- Sufficient "backup" UPS devices are available (to be used when a "primary" UPS unit has 10% or less power remaining) to provide a minimum of 24 hours of power to each critical hardware system.

To ensure that UPS devices within IT remain charged, they must be firmly affixed to power outlets in such a way that they cannot be removed accidentally or by company cleaners, etc.

10.2.1 UPS Devices

UPS devices used in the IT Department must:

- Switch automatically to back-up power in the event of a power failure.
- Be clearly visible and clearly labelled.
- Be tested in accordance with the manufacturer's instructions but no less frequently than once every three months, at times that are not operationally critical, to ensure that they are in working order, and a record of such tests shall be made and signed by the Executive Manager Information Technology.

10.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

10.4 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



11. Vendor Management Procedure

11.1 Introduction

11.1.1 Purpose

The purpose of this procedure is to define suitable vendor access to Company offices and information services, and to define vendor responsibilities for the protection of Company information.

11.1.2 Scope

This procedure is relevant to all staff, contractors, consultants and temporary workers, to ensure that all vendors are managed appropriately and that all information is accessed in a secure and confidential manner.

11.1.3 Enquiries and Faults

Adherence to this procedure will generally ensure compliance with Air Niugini requirements. However, there may be instances where inadvertent breaches could occur. When in doubt, employees requiring assistance with interpretation of this procedure, or who wish to report a breach of this procedure, should contact the Manager, Information Technology.

11.1.4 Responsibility

Vendors play an important role in the support of hardware and software management, and operations for Company. Vendors must comply with all applicable Company policies, procedures and work instructions, including but not limited to:

- Occupational Health and Safety.
- Information Technology Policy.
- Security Policies.
- Code of Conduct and/or Code of Ethics.

11.2 Procedure

11.2.1 Appropriate Vendor Conduct

The vendor must use Company information and IT resources only for the purpose of the relevant business agreement.

Any other Company information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

The vendor must at all times:

- Ensure the security and confidentiality of Company information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorised access to or use of such information that could result in substantial harm or inconvenience to the Company.
- Dispose of confidential customer information in a secure manner.
- Immediately inform the appropriate personnel in the event of a security breach involving confidential Company information.

11.2.2 Prohibited Vendor Conduct

Vendors must not:

- Store and/or access information on Company IT facilities that could result in legal action against the Company.
- View, disseminate, store, share or create any material that is pornographic, lewd, obscene, offensive or discriminatory is prohibited. This includes, but is not limited to, video files, images, documents and email content.
- Use Company IT facilities for transmitting, obtaining, possessing, demonstrating, advertising or requesting the transmission of objectionable material as described above.
- Store any file on the Company's computing network that is subject to copyright protection, without suitable written consent of the licence holder.
- Knowingly possess, give to another person, install or run on any of the computing and networking facilities programs or other information that could result in the violation of any Company policy or the violation of any applicable licence or contract. This is directed towards, but not limited to, software known as viruses, Trojan horses, worms and password breakers.

11.2.3 Vendor Agreements

Vendor agreements and contracts must specify:

- Company information that the vendor should have access to, and how Company information is to be protected by the vendor.
- Acceptable methods for the return, destruction or disposal of Company information in the vendor's possession at the end of the contract.
- That the Company will provide an IT representative for the vendor. The representative will work with the vendor to ensure the vendor complies with these policies.
- Each vendor must provide the Company with a list of all employees working on the contract. The list must be updated and provided to Company within 24 hours of staff changes.
- Vendor personnel must report all breaches of IT security incidents directly to the Manager Information Policy.
- Vendors must follow all applicable Company change control processes and procedures.
- Regular work hours and duties will be defined in the vendor agreement or contract. Work outside of defined parameters must be approved in writing by Executive Manager Information Technology.
- All vendor maintenance equipment on the Company network that connects to the outside world via the network, telephone line or leased line, and all Company vendor accounts, will remain disabled except when in use for authorised maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the Company's requirements. Vendors' major work activities must be entered into a log and be available to Company management upon request.

Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Company or destroyed within 24 hours.

Upon termination of the contract or at the request of the Company, the vendor will return or destroy all Company information and surrender all Company identification badges, access cards, equipment and supplies immediately.

Vendors are required to comply with all legislative and Company auditing requirements, including the auditing of vendor's work.

All software used by the vendor in providing services to Company must be properly inventoried and licensed.

11.2.4 Records

All records of the email system, network services and associated systems will remain the property of Company.

11.3 Procedure Review

This procedure will be reviewed annually or as required to reflect changes in business practice or legislation.

11.4 Authority and Responsibility

This policy is issued under the authority of the Executive Manager Information Technology.



12. Business Continuity Plan

12.1 Introduction

The purpose of a Business Continuity Plan (BCP) is to provide a plan for the continuation of IT services within a required timeframe in the event of any unplanned interruptions.

An Information Technology Business Continuity Plan contains guidelines, procedures and supporting reference material to support continued business operations in the event of an unplanned interruption to Information Technology services.

When a disruption occurs, the Business Continuity Plan is carried out in three steps:

1. Response.
2. Continuation of critical services.
3. Recovery and restoration.

12.1.1 Response

Incident response involves the deployment of teams, plans, measures and arrangements. The following tasks are accomplished during the response phase:

- Incident management.
- Communications management.
- Operations management.

Incident Management

Incident management includes the following measures:

- Notifying management, employees, and other stakeholders.
- Assuming control of the situation.
- Identifying the range and scope of damage.
- Implementing plans.
- Identifying infrastructure outages.
- Coordinating support from internal and external sources.

Communications Management

Communications management is essential to control rumours, maintain contact with the media, emergency services and vendors, and assure employees, the public and other affected stakeholders. Communications management requirements may necessitate building redundancies into communications systems and creating a communications plan to adequately address all requirements.

Operations Management

An Emergency Control Centre (ECC) can be used to manage operations in the event of a disruption. Having a centralised ECC where information and resources can be coordinated, managed and documented helps ensure effective and efficient response.

12.1.2 Continuation of Critical Services

This stage ensures that all time-sensitive critical services or products are continuously delivered or not disrupted for longer than is permissible.

12.1.3 Recovery and Restoration

The goal of recovery and restoration operations is to, recover the facility or operation and maintain critical service or product delivery. Recovery and restoration includes:

- Re-deploying personnel.
- Deciding whether to repair the facility, relocate to an alternate site or build a new facility.
- Acquiring the additional resources necessary for restoring business operations.
- Re-establishing normal operations.
- Resuming operations at pre-disruption levels.

12.2 Objectives

The objectives of this BCP are to focus on the continuation of critical business functions in the event of disruptions, and to establish ways to minimise the effect of unplanned business interruptions.

Further objectives are:

- Ensure that maximum possible service levels are maintained.
- Ensure that the Company recovers from any interruptions as quickly as possible.
- Ensure that critical functions are recovered first, as the business impact of losing them is the greatest.
- Minimise the likelihood and impact (risk) of interruptions.
- Ensure that critical information technology systems, data and processes are identified and appropriate disaster recovery arrangements are established.

Air Niugini acknowledges that business continuity is a key consideration in maintaining and achieving its financial and operational objectives.

12.3 Process

Executive Manager Information Technology is responsible for developing a suitable Information Technology Business Continuity Plan that:

- Includes plans, measures and arrangements to ensure the continuous delivery of critical IT services and products.
- Identifies necessary IT resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodation.

The developed IT Business Continuity Plan shall:

1. Include the following five sections:
 - BCP Governance – refer to Section 12.3.1 *BCP Governance*.
 - Business Impact Analysis (BIA) – refer to Section 12.3.2 *Business Impact Analysis*.
 - Plans, measures, and arrangements for business continuity – refer to Section 12.3.3 *Plans for Business Continuity*.
 - Readiness procedures – refer to Section 12.3.4 *Readiness Procedures*.
 - Quality assurance techniques (exercises, maintenance and auditing) – refer to Section 12.3.5 *Quality Assurance Techniques*.
2. Be tested, reviewed and (as required) updated by the Executive Manager Information Technology by no later than the end of September each calendar year.

12.3.1 BCP Governance

A BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities.

The BCP senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP. It also implements the BCP, coordinates activities, approves the BIA survey, oversees the creation of continuity plans and reviews the results of quality assurance activities. Senior managers or a BCP Committee would normally:

- Approve the governance structure.
- Clarify their roles, and those of participants in the program.
- Oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan.
- Provide strategic direction and communicate essential messages.
- Approve the results of the BIA.
- Review the critical services and products that have been identified.
- Approve the continuity plans and arrangement.
- Monitor quality assurance activities.
- Resolve conflicting interests and priorities.

This BCP committee is normally comprised of the following members:

- Executive sponsor has overall responsibility for the BCP committee. elicits senior management's support and direction. and ensures that adequate funding is available for the BCP program.
- BCP Coordinator secures senior management's support. estimates funding requirements. develops BCP policy. coordinates and oversees the BIA process. ensures effective participant input. coordinates and oversees the development of plans and arrangements for business continuity. establishes working groups and teams and defines their responsibilities. coordinates appropriate training. and provides for regular review, testing and audit of the BCP.
- Security Officer works with the coordinator to ensure that all aspects of the BCP meet the security requirements of the organisation.
- Chief Information Officer (CIO) cooperates closely with the BCP coordinator and IT specialists to plan for effective and harmonised continuity.
- Business unit representatives provide input, and assist in performing and analysing the results of the business impact analysis.

The BCP committee is commonly co-chaired by the executive sponsor and the coordinator.

NOTE: In a corporate emergency response situation, the BCP senior management committee is the Company Response Management Team – refer to Section 12.4 *Response Management Team (RMT)*.

12.3.2 Business Impact Analysis (BIA)

The purpose of the BIA is to identify the organisation's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

12.3.2.1 Identify the Mandate and Critical Aspects of an Organisation

This step determines what goods or services it must be delivered. Information can be obtained from the mission statement of the organisation, and legal requirements for delivering specific services and products.

12.3.2.2 Prioritise Critical Services Or Products

Once the critical services or products are identified, they must be prioritised based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organisation results. To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

12.3.2.3 Identify Impacts of Disruptions

The impact of a disruption to a critical service or business product determines how long the organisation could function without the service or product, and how long clients would accept its unavailability. It will be necessary to determine the time period that a service or product could be unavailable before severe impact is felt.

12.3.2.4 Identify Areas of Potential Revenue Loss

To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue. If these processes and functions are not performed, is revenue lost? How much? If services or goods cannot be provided, would the organisation lose revenue? If so, how much revenue, and for what length of time? If clients cannot access certain services or products would they then go to another provider, resulting in further loss of revenue?

12.3.2.5 Identify Additional Expenses

If a business function or process is inoperable, how long would it take before additional expenses would start to add up? How long could the function be unavailable before extra personnel would have to be hired? Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties?

12.3.2.6 Identify Intangible Losses

Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations. Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards.

12.3.2.7 Insurance Requirements

Since few organisations can afford to pay the full costs of a recovery, having insurance ensures that recovery is fully or partially financed.

When considering insurance options, decide what threats to cover. It is important to use the BIA to help decide both what needs insurance coverage, and the corresponding level of coverage. Some aspects of an operation may be overinsured, or underinsured. Minimise the possibility of overlooking a scenario, and to ensure coverage for all eventualities.

Document the level of coverage of your institutional policy, and examine the policy for uninsured areas and non specified levels of coverage. Property insurance may not cover all perils (steam explosion, water damage, and damage from excessive ice and snow not removed by the owner). Coverage for such eventualities is available as an extension in the policy.

When submitting a claim, or talking to an adjustor, clear communication and understanding is important. Ensure that the adjustor understands the expected full recovery time when documenting losses. The burden of proof when making claims lies with the policyholder and requires valid and accurate documentation.

Include an expert or an insurance team when developing the response plan.

12.3.2.8 Ranking

Once all relevant information has been collected and assembled, rankings for the critical business services or products can be produced. Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause. Minimum service levels and maximum allowable downtimes are then determined.

12.3.2.9 Identify Dependencies

It is important to identify the internal and external dependencies of critical services or products, since service delivery relies on those dependencies.

Internal dependencies include employee availability, corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and support services such as finance, human resources, security and information technology support.

External dependencies include suppliers, any external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service.

12.3.3 Plans for Business Continuity

This step consists of the preparation of detailed response/recovery plans and arrangements to ensure continuity. These plans and arrangements detail the ways and means to ensure critical services and products are delivered at a minimum service levels within tolerable down times. Continuity plans should be made for each critical service or product.

12.3.3.1 Mitigating Threats and Risks

Threats and risks are identified in the BIA or in a full-threat-and-risk assessment. Moderating risk is an ongoing process, and should be performed even when the BCP is not activated. For example, if an organisation requires electricity for production, the risk of a short term power outage can be mitigated by installing stand-by generators.

Another example would be an organisation that relies on internal and external telecommunications to function effectively. Communications failures can be minimised by using alternate communications networks, or installing redundant systems.

12.3.3.2 Analyse Current Recovery Capabilities

Consider recovery arrangements the organisation already has in place, and their continued applicability. Include them in the BCP if they are relevant.

12.3.3.3 Create Continuity Plans

Plans for the continuity of services and products are based on the results of the BIA. Ensure that plans are made for increasing levels of severity of impact from a disruption. For example, if limited flooding occurs beside an organisation's building, sand bagging may be used in response. If water rises to the first floor, work could be moved to another company building or higher in the same building. If the flooding is severe, the relocation of critical parts of the business to another area until flooding subsides may be the best option.

Another example would be a company that uses paper forms to keep track of inventory until computers or servers are repaired, or electrical service is restored. For other institutions, such as large financial firms, any computer disruptions may be unacceptable, and an alternate site and data replication technology must be used.

The risks and benefits of each possible option for the plan should be considered, keeping cost, flexibility and probable disruption scenarios in mind. For each critical service or product, choose the most realistic and effective options when creating the overall plan.

12.3.3.4 Response Preparation

Proper response to a crisis for the organisation requires teams to lead and support recovery and response operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

The number and scope of teams will vary depending on organisation's size, function and structure, and can include:

- Emergency Control Centre that includes a Response Management Team.
- Task Oriented Teams that include an Alternate Site Coordination Team, Contracting and Procurement Team, Damage Assessment and Salvage Team, Finance and Accounting Team, Hazardous Materials Team, Insurance Team, Legal Issues Team, Telecommunications/ Alternate Communications Team, Mechanical Equipment Team, Mainframe/ Midrange Team, Notification Team, Personal Computer/ Local area Network Team, Public and Media Relations Team, Transport Coordination Team and Vital Records Management Team

The duties and responsibilities for each team must be defined, and include identifying the team members and authority structure, identifying the specific team tasks, member's roles and responsibilities, creation of contact lists and identifying possible alternate members.

For the teams to function in spite of personnel loss or availability, it may be necessary to multitask teams and provide cross-team training.

12.3.3.5 Alternate Facilities

If an organisation's main facility or Information Technology assets, networks and applications are lost, an alternate facility should be available. There are three types of alternate facility:

1. Cold site is an alternate facility that is not furnished and equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and a substantial time and effort is required to make a cold site fully operational. Cold sites are the least expensive option.
2. Warm site is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. Warm sites are more expensive than cold sites.
3. Hot site is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds. Hot sites are the most expensive option.

When considering the type of alternate facility, consider all factors, including threats and risks, maximum allowable downtime and cost.

For security reasons, some organisations employ hardened alternate sites. Hardened sites contain security features that minimise disruptions. Hardened sites may have alternate power supplies, back-up generation capability, high levels of physical security, and protection from electronic surveillance or intrusion.

12.3.4 Readiness Procedures

12.3.4.1 Training

Business continuity plans can be smoothly and effectively implemented by:

- Having all employees and staff briefed on the contents of the BCP and aware of their individual responsibilities
- Having employees with direct responsibilities trained for tasks they will be required to perform, and be aware of other teams' functions

12.3.4.2 Exercises

After training, exercises should be developed and scheduled in order to achieve and maintain high levels of competence and readiness. While exercises are time and resource consuming, they are the best method for validating a plan. The following items should be incorporated when planning an exercise:

Goal	The part of the BCP to be tested.
Objectives	The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely.
Scope	Identifies the departments or organisations involved, the geographical area, and the test conditions and presentation.
Artificial aspects and assumptions	Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.
Participant Instructions	Explains that the exercise provides an opportunity to test procedures before an actual disaster.
Exercise Narrative	Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions.
Communications for Participants	Enhanced realism can be achieved by giving participants access to emergency contact personnel who share in the exercise. Messages can also be passed to participants during an exercise to alter or create new conditions.
Testing and Post-Exercise Evaluation	The exercise should be monitored impartially to determine whether objectives were achieved. Participants' performance, including attitude, decisiveness, command, coordination, communication, and control should be assessed. Debriefing should be short, yet comprehensive, explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation.

Exercise complexity level can also be enhanced by focusing the exercise on one part of the BCP instead of involving the entire organisation.

12.3.5 Quality Assurance Techniques

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. It should also uncover which aspects of a BCP need improvement. Continuous appraisal of the BCP is essential to maintaining its effectiveness. The appraisal can be performed by an internal review, or by an external audit.

12.3.5.1 Internal Review

It is recommended that the BCP is reviewed:

- On a regular basis (annually or bi-annually).
- When changes to the threat environment occur;
- When substantive changes to the organisation take place.
- After an exercise, to incorporate findings.

12.3.5.2 External Audit

When auditing the BCP, consultants nominally verify:

- Procedures used to determine critical services and processes.
- Methodology, accuracy, and comprehensiveness of continuity plans.

12.4 Response Management Team (RMT)

If a major incident or disaster occurs, the Response Management Team (RMT) will be convened and the situation will be assessed. It will be the responsibility of the RMT to decide whether or not to implement a Corporate Business Continuity Plan. The Information Technology Business Continuity Plan would be one component of such a Corporate Business Continuity Plan.

For further information about the Response Management Team and Air Niugini's corporate emergency response procedures, refer to the Emergency Response Manual.

When an emergency has been declared by the RMT, the Executive Manager Information Technology will report directly to the RMT at the Emergency Control Centre (ECC) for instructions and guidance.. All ad hoc requests during the emergency situation for Information Technology information, decisions, assistance with facilities, acquiring outside services, etc. will be directed by the Executive Manager Information Technology.





13. Appendix A – Staff Responsibility

13.1 Damaged, Lost, or Stolen Assets

Staff must report all damaged, lost or stolen assets to their immediate manager and the IT Service Desk. A Police report must be provided for company issued assets which have been stolen, for review and consideration by Management for custodian to possibly be exempted from reimbursing Air Niugini Limited for the loss.

IT Service Desk must report the incident to their Executive Manager, and Finance Payroll department immediately. Employees, who have lost or damaged the company issued asset, will reimburse Air Niugini Limited through salary deduction for the asset and any associated equipment that may have been provided as per their current book value. Air Niugini Finance department will set the current book value of the asset with the associated equipment.

IT Service Desk must ensure amendments are made to the IT asset register of the company issued assets, to reflect the correct status of the asset in such circumstances.

13.2 Employees Leaving or Internal Transfer

Employees must return their company issued assets and any associated equipment to IT Service Desk before they leave the employment of Air Niugini Limited.

Employees, who leave the company without returning any company issued asset in their custody, will reimburse Air Niugini Limited through their final payments for the asset and any associated equipment that may have been provided as per their current book value. Air Niugini Finance department will set the current book value of the asset with the associated equipment.





Document Change Request

It is very important to have up-to-date and correct information in our manuals. They are the tools we use to ensure safety, reliability and compliance within the airline, and they set the foundation for building a quality work ethic.

All Air Niugini manuals are living documents that need to be changed and added to from time to time.

To help you tell us about changes and additions that are needed to this manual, a *Document Change Request* Form is provided on the following pages.

Instructions

The *Document Change Request* Form is printed on the following pages. Always photocopy both sides of the form, complete the photocopies and have them signed by your manager. Your manager will give you a signed copy back and will forward the original signed copy to the Document Owner.

Do not write on the original printed form. Always return it to its correct place in this manual after copying it.





DOCUMENT CHANGE REQUEST

Document Title:

1. Brief description of change:

2. Reason:

3. Page number(s) requiring amendment:

(Attach photocopies of pages with handwritten amendments or provide an electronic copy of the amended pages).

4. Name: 6. Title:

5. Signed: 7. Date:

COMPLIANCE CHECKS by RESPECTIVE DEPARTMENT: Department Name:

Compliance Manager – Name:

Signed: Date:

Change Authority – Name:

Signed: Date:

DOCUMENT OWNER'S APPROVAL: I have reviewed this amendment and it is approved.

Name: Title:

Signed: Date:

Please tick one: CASA PNG Approval Required. CASA PNG Acceptance Required.

CASA PNG Approval / Acceptance Not Required.

DOCUMENT PRODUCTION USE ONLY:

Date Received: New Version Number: Date DCR Actioned:

Quarterly Publishing Cycle: Tick One

1st Quarter (1 January) 2nd Quarter (1 April) 3rd Quarter (1 July) 4th Quarter (1 October)

Originator Document Owner

The Document Change Request you raised / approved has been registered. For further enquires, refer to DCR No:



Air Niugini