

GenOmega

Achieving the Genesis and Omega



GenOmega Partners

Standard Operating Environment

Volume 9:

Security & Risk Management Policies

for

XYZ Pty Ltd



Document Authorisation

Author: Mr / Ms
Title: Head, Fraud and Operating Risk Management
Telephone: +61-3-
Fax: +61-3-
Approved by:
Title: Chief Information Officer
Published by: XYZ Pty Ltd
Telephone: +61-3-
Application: Internet Banking
Distribution Details:

Record of Issues

Issue No	Issue Date	Nature of Amendment
1.0	05/05/2001	Ratified and Released

This publication has been prepared for XYZ P/L, and is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, micro copying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission from the document controller. Product or company names are trademarks or registered trademarks of their respective holders.

Note for non-XYZ readers: The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, XYZ does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.



Contents

DOCUMENT AUTHORISATION.....	2
FOREWORD.....	6
1. INTRODUCTION.....	7
1.1. PURPOSE	7
1.2. IT SECURITY POLICY APPROACH.....	7
1.3. OBJECTIVES	8
1.4. SCOPE	8
1.5. POLICY APPLICATION	8
1.6. PERSONNEL COVERED BY THIS IT SECURITY POLICY	9
1.7. POLICY COMPLIANCE.....	9
1.8. RESPONSIBILITY.....	9
1.9. LEGISLATIVE AND LEGAL COMPLIANCE	9
1.10. UPDATES.....	10
1.11. RISK MANAGEMENT FRAMEWORK	10
2. IT SECURITY MANAGEMENT.....	11
2.1. INTRODUCTION	11
2.2. OPERATING RISK MANAGEMENT AND AUDIT COMMITTEE (ORMAC).....	13
2.3. IT SECURITY COMMITTEE (SC)	13
2.4. SECURITY MANAGER.....	14
2.5. XYZ HELP DESK	15
2.6. BUSINESS UNIT MANAGERS.....	16
2.7. XYZ PERSONNEL.....	16
3. POLICY STRUCTURE	17
3.1. IT SECURITY POLICY DOCUMENT STRUCTURE	17
3.2. STRUCTURE - IT SECURITY POLICIES.....	18
3.3. SECURITY POLICY OBJECTIVES.....	18
3.4. SECURITY RATIONALE	18
3.5. SECURITY STANDARDS	18
3.6. DEVIATION FROM POLICY AND STANDARD FORMS.....	18
4. ACCEPTABLE USE POLICIES.....	19
4.1. IT RESOURCES.....	19
4.2. ELECTRONIC MAIL POLICY	21
5. CORPORATE SECURITY POLICIES.....	24
5.1. ACCESS CONTROL - DEFINITIONS	24
5.2. ACCESS CONTROL – USER REGISTRATION.....	25
5.3. ACCESS CONTROL – SYSTEM ADMINISTRATION	25
5.4. ACCESS CONTROL – USER ADMINISTRATION	27
5.5. ACCESS CONTROL – REMOTE ACCESS	29
5.6. ACCESS CONTROL – PRIVILEGED ADMINISTRATION.....	30
5.7. SECURE MANAGEMENT OF SOFTWARE	30
5.8. SOFTWARE – SYSTEM LIFE CYCLE	31
5.9. PHYSICAL SECURITY	32



5.10.	HARDWARE IDENTIFICATION	32
5.11.	NETWORK AND COMMUNICATIONS SECURITY	33
5.12.	BACKUP	34
5.13.	DISASTER RECOVERY AND CONTINGENCY PLANNING	35
6.	HOSTING PARTY POLICIES	37
6.1.	COMPUTER NETWORK SECURITY POLICY	37
6.2.	SUPPORT STAFF IMPLICATIONS	37
6.3.	REGULATION OF SPECIAL ACCESS	38
6.4.	AUDIT OF HIGH LEVEL SYSTEM ACCESS	39
6.5.	CULLING THE SPECIAL ACCESS DATABASE	39
6.6.	ESCALATION OF SECURITY INCIDENTS	40
6.7.	REMOTE ACCESS	40
7.	FIREWALL POLICIES	41
7.1.	FIREWALL PURPOSE	41
7.2.	AUTHENTICATION	41
7.3.	FIREWALL SELECTION AND IMPLEMENTATION	42
7.4.	APPLICATION LEVEL FIREWALL SERVICES	43
7.5.	FIREWALL ARCHITECTURES	44
7.6.	MULTI-HOMED HOST FIREWALL	44
7.7.	SCREENED HOST FIREWALL	44
7.8.	SCREENED SUBNET FIREWALL	45
7.9.	INTRANET POLICY	45
7.10.	FIREWALL ADMINISTRATION POLICY	46
7.11.	QUALIFICATION OF THE FIREWALL ADMINISTRATOR	46
7.12.	REMOTE FIREWALL ADMINISTRATION	46
7.13.	USER ACCOUNTS	47
7.14.	FIREWALL BACKUP	48
7.15.	SYSTEM INTEGRITY	48
7.16.	INTRUSION DETECTION	49
7.17.	NETWORK TRUST RELATIONSHIP	49
7.18.	VIRTUAL PRIVATE NETWORKS (VPN)	50
7.19.	DNS AND MAIL RESOLUTION	50
7.20.	PHYSICAL FIREWALL SECURITY	51
7.21.	FIREWALL INCIDENT HANDLING	51
7.22.	RESTORATION OF SERVICES	51
7.23.	UPGRADING THE FIREWALL	52
7.24.	REVISION/UPDATE OF FIREWALL POLICY	52
7.25.	LOGS AND AUDIT TRAILS	53
7.26.	DOCUMENTATION	54
7.27.	ENVIRONMENT POLICIES	54
8.	INTERNET	58
8.1.	INTRODUCTION	58
8.2.	INTERNET POLICY	58
8.3.	INTRANET/EXTRANET	59
8.4.	INFORMATION INTEGRITY	60
8.5.	PUBLIC REPRESENTATIONS	61
8.6.	INTELLECTUAL PROPERTY RIGHTS	62
8.7.	ACCESS CONTROL	63
8.8.	OWNERSHIP	63
8.9.	REPORTING SECURITY PROBLEMS	64



9. MANAGING SECURITY INCIDENTS	66
9.1. INTRODUCTION	66
9.2. SECURITY INCIDENT DEFINITION	66
9.3. AREAS OF RESPONSIBILITY	66
9.4. EMERGENCY PLANS	66
9.5. PROCEDURES TO MANAGE A SECURITY INCIDENT	66
9.6. RELEASE OF INFORMATION	68
9.7. TRACKING INCIDENTS	68
10. RISK MANAGEMENT FRAMEWORK	69
10.1. INTRODUCTION	69
10.2. RISK IDENTIFICATION	69
10.3. ASSESSMENT OF RISK(S).....	71
10.4. TREATMENT OF RISK	73
10.5. DEVIATION FROM POLICY AND STANDARDS	74
10.6. RISK REGISTER	74
10.7. PROCESS SUMMARY.....	74
APPENDIX A. RISK MANAGEMENT FRAMEWORK	76
A.1. DESCRIPTION OF IT VULNERABILITIES	76
APPENDIX B. REQUEST FOR DEVIATION	81
APPENDIX C. RISK REGISTER	82
INDEX	83



Foreword

XYZ Pty Ltd (herein referred to in this document as XYZ) has a duty to protect its information and information processing technology, as both are critical to the success of XYZ's corporate strategies.

XYZ IT management team is committed to ensuring the protection of the Group's information and IT assets, and, to provide the same level of protection to customer, business and alliance partner's information that is stored, processed, transmitted or otherwise controlled by XYZ on their behalf.

XYZ has a legal, moral and commercial obligation to take the necessary steps to ensure that the Group's corporate information, and IT environment used to process that information, is protected from security threats, including:

- Unauthorised access to computer systems, including hacking;
- Malicious code, including viruses;
- Data theft;
- Unauthorised data manipulation;
- Human error;
- Fraud;
- Sabotage;
- Industrial espionage;
- Privacy violation;
- Service interruption; and,
- Natural disaster.

To achieve XYZ's IT Security objectives, all personnel must actively acknowledge their responsibility to secure and protect XYZ information and technology. XYZ management must ensure that sufficient funds, resources and time are devoted to IT Security and the protection of information.

XYZ has developed this IT Security Policy document which contains practical security standards, procedures and guidelines to protect the confidentiality, integrity and availability of electronic information stored and processed by our IT systems.

Chief Executive Officer

Chief Information Officer